

carahsoft

CARASOFT'S RESPONSE TO THE

**State of North Carolina Department
of Information Technology**

REQUEST FOR PROPOSAL

Enterprise Electronic Forms and Digital Signature Capability

SOLICITATION NO. ITS-400335

Tuesday
July 24, 2018

SOLUTION PROVIDED BY

DocuSign®

CARASOFT TECHNOLOGY CORP.
1860 MICHAEL FARADAY DRIVE, SUITE 100
RESTON, VA 20190

888.66.CARAH | WWW.CARASOFT.COM

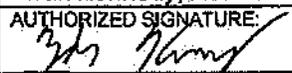
© Copyright DocuSign, Inc., 2018. All rights reserved. This document contains DocuSign, Inc., confidential and proprietary information. Use of any part of this document without the express written consent of DocuSign, Inc. is prohibited. DocuSign is a registered trademark of DocuSign, Inc. All other trademarks are property of their respective owners. PROPRIETARY DATA: This data, furnished to the State of North Carolina Department of IT shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed in whole or in part for any purpose other than evaluation; provided, that if a contract is awarded to this Offeror as a result of or in connection with the submission of this data, the Government shall have the right to duplicate, use, or disclose this data to the extent provided in the contract. This restriction does not limit the Government's right to use information contained in the data without restriction if it is obtained from another source. The data subject to this restriction is contained in sheets marked with a data restriction legend in the page footer.

STATE OF NORTH CAROLINA Department of Information Technology	REQUEST FOR PROPOSAL NO. ITS-400335	
	Offers will be publicly opened: July 12, 2018	
Refer ALL inquiries regarding this RFP to: Kristen Burnette kristen.burnette@nc.gov 919-754-6678	Issue Date: June 11, 2018	
	Commodity Number: 208	
	Description: Enterprise Electronic Forms and Digital Signature Capability	
See page 2 for mailing instructions.	Using Agency: Multiple State Agencies	
	Requisition No.: NA	

OFFER AND ACCEPTANCE: The State seeks offers for the Online Services and/or goods described in this solicitation. All offers and responses received shall be treated as offers to contract. The State's acceptance of any offer must be demonstrated by execution of the acceptance found below, and any subsequent Request for Best and Final Offer, if issued. Acceptance shall create a contract having an order of precedence as follows: Best and Final Offers, if any, Special terms and conditions specific to this RFP, Specifications of the RFP, the Department of Information Technology Terms and Conditions, and the agreed portion of the awarded Vendor's offer.

EXECUTION: In compliance with this Request for Proposal, and subject to all the conditions herein, the undersigned offers and agrees to furnish any or all Services or goods upon which prices are offered, at the price(s) offered herein, within the time specified herein. By executing this offer, I certify that this offer is submitted competitively and without collusion.

Failure to execute/sign offer prior to submittal shall render offer invalid. Late offers are not acceptable.

OFFEROR: Carahsoft Technology Corporation		
STREET ADDRESS: 1860 Michael Faraday Drive, Suite 100	P.O. BOX:	ZIP: 20190
CITY, STATE & ZIP: Reston, VA 20190	TELEPHONE NUMBER: 703-871-8500	TOLL FREE TEL. NO. 888-662-2724
PRINT NAME & TITLE OF PERSON SIGNING: Zak Kennedy, Account Representative	FAX NUMBER: 703-871-8505	
AUTHORIZED SIGNATURE: 	DATE: 7/23/18	E-MAIL: Zak.Kennedy@carahsoft.com

Offer valid for ninety (90) days from date of offer opening unless otherwise stated here: ___ days.

ACCEPTANCE OF OFFER: If any or all parts of this offer are accepted, an authorized representative of AGENCY shall affix their signature hereto and this document and the documents identified above shall then constitute the written agreement between the parties. A copy of this acceptance will be forwarded to the awarded Vendor(s).

FOR AGENCY USE ONLY
Offer accepted and contract awarded _____, as indicated on attached certification, by _____ (Authorized representative of DEPARTMENT OF INFORMATION TECHNOLOGY).

carahsoft.

A. LETTER OF TRANSMITTAL

July 24, 2018

Department of Information Technology
3900 Wake Forest Road
Raleigh, NC 27609

Re: Carahsoft's Response to the State of North Carolina Department of Information Technology's Request for Proposal for Enterprise Electronic Forms and Digital Signature Capability, Solicitation # ITS-400335

Dear Ms. Burnette,

Carahsoft Technology Corp. appreciates the opportunity to respond to the State of North Carolina Department of Information Technology (State)'s Request for Proposals for Enterprise Electronic Forms and Digital Signature Capability. Carahsoft is proposing DocuSign which fully meets the State's requirements. Our team has fully considered the State's requirements outlined in the Request for Proposals and has carefully put together a solution that will best meet your needs.

Requested Information:

- i. **Submitting organization:** Carahsoft Technology Corporation
- ii. **Contact for contractual obligations:** Zak Kennedy
- iii. **Contact for person authorized to negotiate for Carahsoft:** Zak Kennedy
- iv. **Contact for clarifications:** Jacob Holler
- v. **Acknowledgement of Amendments:** Carahsoft acknowledges Addendums 1, 2, and 3.

Please feel free to contact me directly at 703.581.6581/Jacob.Holler@carahsoft.com or Zak Kennedy at 703.230.7430/Zak.Kennedy@carahsoft.com with any questions or communications that will assist the State in the evaluation of our response. This proposal is valid for 90 days from the date of submission.

Thank you for your time and consideration.

Sincerely,

Jacob Holler
Account Representative

B. TABLE OF CONTENTS

A. Letter of Transmittal	3
Executive Summary.....	3
Prime Contractor: Carahsoft Technology Corp.	3
Solution Provider: DocuSign	4
Technical Proposal.....	7
DocuSign's Certifications & Tests	9
C. Response to Technical Specifications	20
1. General Features.....	20
2. Product Strategy Roadmap	28
Support & Self-Service Resources.....	30
State of North Carolina's 12-month Plan	31
3. Disaster Recovery and Hosting Facilities	37
4. Data Management	40
5. Audit.....	41
6. NCID.....	43
7. Architecture	47
8. Interoperability and Integration	50
9. Applications Management and Control.....	63
10. Application Specifications.....	65
11. Automation of Forms	71
12. Workflow	74
Ability to Change the Workflow	74
13. Signature/Initialing.....	81
14. Repudiation	84
15. Notification	87
16. Storage.....	90
17. Service Level Agreement (SLA) and Reporting.....	92
18. Software Support and Maintenance Services	95

19. Training	102
D. Completed Cost Offer	110
DocuSign's Pricing Response	116
E. References	129
Reference #1	129
Reference #2	129
Reference #3	129
F. Financial Information	130
G. Conflict of Interest	131
H. Errata and Exceptions	132
I. Copy of Vendor's License and Maintenance Agreements	133
K. Other Supporting Material Including Technical System Documentation	189
Questions from Addendum 3 – Q&A	189
DocuSign Policies and Procedures Worksheet	193
K. Training and Other Materials, Samples or Examples	206
Attachments	207
Solicitation	207
Vendor Readiness Assessment Report	275
Addendum 1 Confirmation	326
Addendum 2 Confirmation	328
Addendum 3 Confirmation	330

EXECUTIVE SUMMARY

Detailed description of Vendor's firm should include all of the following:

i) Full name, address, and telephone number of the organization;

Carahsoft Technology Corporation
1860 Michael Faraday Drive, Suite 100, Reston, VA 20190
703-871-8500

ii) Date established;

Incorporated on 10/25/1999.

iii) Background of firm;

Please see the information provided below.

iv) Ownership (public company, partnership, subsidiary, etc.);

Sole ownership of Craig Abod.

v) If incorporated, state of incorporation must be included.

Maryland.

vi) Number of full-time employees on January 1st for the last three years or for the duration that the Vendor's firm has been in business, whichever is less.

2016: 558 employees

2017: 634 employees

2018: 814 employees

Prime Contractor: Carahsoft Technology Corp.

Carahsoft Technology Corp. is an IT solutions provider delivering best-of-breed hardware, software, and support solutions to federal, state and local government agencies since 2004. Carahsoft has built a reputation as a customer-centric real-time organization with unparalleled experience and depth in government sales, marketing, and contract program management. This experience has enabled Carahsoft to achieve the top spot in leading public-sector software license resellers.

VENDOR RELATIONSHIPS – Carahsoft has a unique business model focusing on providing superior sales and marketing execution, a track record of success, high integrity, and a focus on strategic vendor relationships, of which **DocuSign** is an important part.

PROVEN EXECUTION – Carahsoft has leveraged its vast contracting experience and extended it to quoting and order management. Carahsoft seamlessly generates quotes within 30 minutes or less and processed over 85,000 orders in 2017 that were each completed the same day received.

CONTRACT VEHICLES – Over the past 14 years Carahsoft has acquired and maintained a wide variety of purchasing contract vehicles for agencies at the state, local, and federal levels. Associated with all contracts are dedicated and experienced contract management resources. A list of available contracts can be found at www.carahsoft.com/contracts/index.php.

GROWTH & STABILITY – Carahsoft has continued to show impressive growth year after year, with annual revenue of \$3.4 million in our first year in 2004 to \$4.4 billion in 2017. In September of 2017, 10,705 orders were processed worth over \$1 billion. We are a stable, conservative, and profitable company and have received numerous accolades, as detailed on our awards page: <http://www.carahsoft.com/awards>.

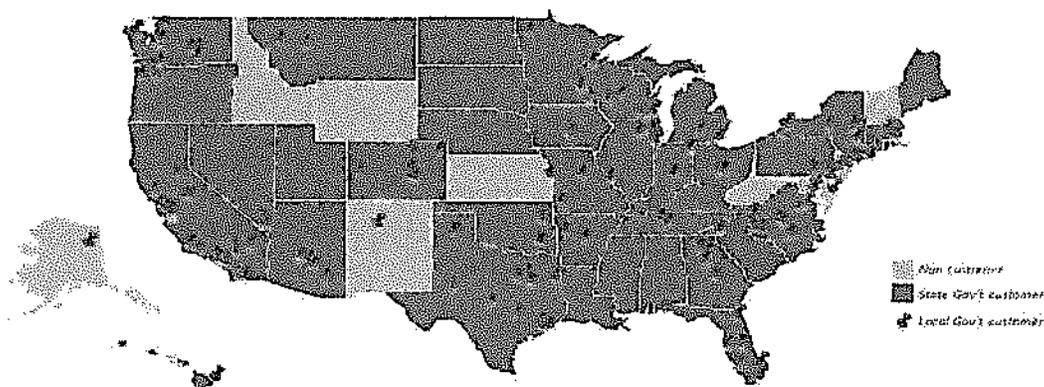
Solution Provider: DocuSign

DocuSign DocuSign, founded in 2003, is changing how business gets done by empowering more than 400,000 companies and hundreds of millions of users across 180+ countries to sign, send and manage documents anytime, anywhere, on any device, with confidence. DocuSign replaces printing, faxing, scanning and overnighting documents with the easiest, fastest, most trusted way to make every approval and decision digital. Organizations of all sizes and industries are accelerating contracts, approvals, and workflows with DocuSign's System of Agreement (SofA) platform. DocuSign accelerates and simplifies how companies prepare, sign, enact, and manage agreements.

DocuSign meets the needs of a wide range of government services. Over the years, DocuSign has proven success with government agencies, such as Santa Clara County, City and County of San Francisco, Illinois Public Health, multiple school districts and institutions of higher education. They have standardized on DocuSign for eSignatures and e-forms across the enterprise, automating processes such as renewals and contracts for Purchasing Department, travel reimbursements and notice of personnel action for Department of Health, ITD and auction transfer for Information Technology Department, and many more. DocuSign's customer list includes global firms and industry leaders such as Microsoft, HP, SAP, Apple, Google, as well as over 600 Federal, State and Local agencies such as the Internal Revenue Service (IRS), Department of Veteran's Affairs, State of Virginia, Nevada DOT, State of California, Boulder County, CO, State of Illinois, State of Texas, and thousands more. As shown below, DocuSign's expertise in the government marketplace is broad and deep. Team DocuSign offers the State the best-in-class solution to transform the way your district functions. By further integrating DocuSign into the State's process, your state employees and constituents and will benefit from an enhanced experience with lower risk, thus providing significant benefit and value to the state agencies.

As shown below, DocuSign's expertise in the government marketplace is broad and deep.

Public Sector is Embracing DocuSign 39 States and 600+ City, County, and Municipal Organizations



Team DocuSign offers the State the best-in-class solution to transform the way the State does business. By further integrating DocuSign into State agencies' processes, your constituents will benefit from an enhanced customer experience with lower risk, thus providing significant benefit and value to the State.

Our Understanding:

DocuSign understands the State of North Carolina is establishing an Indefinite Quantity Contract for an enterprise electronic forms and digital signatures (EEF & DS) solution. Some of the State's key concerns for this RFP are identity, authentication, confidentiality, data integrity, and non-repudiation. The State is also requiring a rolled-up view of utilization both quarterly and yearly. DocuSign is excited at the prospect of further cementing our relationship with the State as we work together to accomplish these objectives.

The State of North Carolina has been a DocuSign customer since 2012. The State was an early adopter and recognized the need for an electronic signature solution. DocuSign has partnered with many State Agencies, such as the Department of Transportation, Department of Health and Human Services, and at least 10 other agencies to come to agreement faster.

Highlights of DocuSign's solution:

Customized solution to meet the State of NC needs

By partnering with Carahsoft, DocuSign is proposing a flexible billing strategy to meet the needs of DIT and the different agencies within the State of North Carolina. For the current process, DocuSign sends a quote, the State pays DocuSign, and then will the State will charge back to the agencies.

Team DocuSign is proposing an easier solution which will reduce the administrative burden on the State. The new process will be initiated by DocuSign sending a quote to Carahsoft, who will bill the agencies directly.

New Administration Features makes life easy for DIT

DocuSign has many new exciting features in the Organizational Management feature which will allow DIT to reduce the time and effort spent on managing the overall contract, thus resulting in cost savings for DIT.

We've added to our Organization Administration features to help companies manage the complexity of scale, compliance and quarterly audits. With Organization Management, DIT can gain centralized management of all their users at an organization level across multiple accounts. DIT can define and leverage flexible and customizable delegated administrative roles, reduce complexity and time on daily tasks and audit reviews with user list exports, and gain full insight into administrative changes and events with organization audit logs.

Customer Success Program developed and tailored for the State

Since 2012, DocuSign has partnered with the State to use DocuSign and identify and implement new use cases. As part of our response, DocuSign has created a targeted Customer Success Program which includes free training based on three main user roles, with a timeline for each of these. It is adaptable for any new agency starting with DocuSign and will enable to them to get up and running with DocuSign with little involvement from DIT.

DocuSign is a trusted provider and partner

Since 2012, DocuSign has partnered with the State. Based on our long-standing relationship with the State, we have worked to meet your needs. There is a history of proven performance, reliability, uptime, and overall a general willingness to meet your needs.

SOLICITATION # ITS-400335

DocuSign leads the industry with the highest breadth and depth of security certifications and auditor assurances, meeting the industry's highest security standards to protect your data and a platform while complying with all security requirements. DocuSign was the first eSignature System of Agreement (SofA) vendor based, in the US, who was FedRAMP authorized. As we are the first to market, the State will also benefit from new features which enhance the experience for your internal agencies and external constituents:

- DocuSign is certified to all 114 optional and mandatory ISO 27001 controls.
- DocuSign is certified to the xDTM Standard, the leading security certification covering Digital Transaction Management platforms.

DocuSign is an enterprise level provider that can scale to meet the needs of the State

DocuSign is the only enterprise grade solution provider. As the leader in the System of Agreement (SofA) and eSignature marketplace, DocuSign provides the greatest depth of product offering, support, and capabilities. DocuSign's over 2,300 employees are all dedicated to the SofA and eSignature, more than five (5) times the nearest competitor. Specifically, we have over 80 in new Product Development, over 80 in Security and IT, and over 500 in Product Support and Customer Success. No other eSignature provider even comes close.

DocuSign supports a platform architecture consisting of three geo-dispersed data centers in the US. Customer data can be replicated across nine (9) different servers. DocuSign is the only vendor that uses carrier-grade platform architecture, with no downtime. To deploy an enterprise solution in a complicated environment, with different agencies and different deployment options, only the industry leader will do.

Availability

DocuSign has invested over \$300 million to build the most powerful DTM platform in the industry. This platform, with more than 99.99% system uptime over the past five years and no scheduled downtime. Some of our competitor's reserve time for maintenance which does not count against their SLA and may have experienced large periods of downtime in the last few months. DocuSign will provide the State the unparalleled availability required to support your mission critical business processes. Please see **Questions from Addendum 3 – Q&A** for specific information on our uptime.

TECHNICAL PROPOSAL

1) **ENTERPRISE ARCHITECTURE STANDARDS:** *The North Carolina Statewide Technical Architecture is located at the following website: (<https://it.nc.gov/services/it-architecture/statewide-architecture-framework>). This provides a series of domain documents describing objectives, principles and best practices for the development, implementation, and integration of business systems. Agencies and Vendors should refer to these Architecture documents when implementing enterprise applications and/or infrastructure.*

Yes, DocuSign's implementation team will be well versed on the documentation provided and will develop a mutually agreed upon plan to incorporate these requirements.

DocuSign will scope each use case and establish a scope outline and schedule as well as any other KPI metrics. The project will be broken down into milestones/sprints where progress can be tracked and measured on regular intervals and appropriate triage and trade off decisions can be made for issues as they may arise.

Our implementation team will provide best practice guidance on how to successfully prepare your organization and DocuSign users for deployment to achieve the highest adoption and ROI value possible. This will include communication emails, meetings, and demonstrations during critical milestones of your implementation. We will also provide executive status reports and success metric tracking post implementation.

2) **ENTERPRISE LICENSING:** *In offering the best value to the State, Vendors are encouraged to leverage the State's existing resources and license agreements. The agreements may be viewed at: <http://it.nc.gov/services/license-and-agreements>*

a) *Identify components or products that are needed for your solution that may not be available with the State's existing license agreement.*

Not applicable.

b) *Identify and explain any components that are missing from the State's existing license agreement.*

The following features are missing from the State's existing license agreement

- E-Notary
- Access Management/Organizational Administration

These features are requirements for use cases with Agencies we already work with in North Carolina that are not included as options in the current agreement between DocuSign and the North Carolina.

c) *If the Vendor can provide a more cost effective licensing agreement, please explain in detail the agreement and how it would benefit the State.*

DocuSign is open to renegotiating an Unlimited usage model based on a DocuSign Platform deal. This would include a platform access fee and a flat fee for sufficient transactions to include all of the States' potential eSignature needs. This type of cost effective licensing agreement will give the State access to all Enterprise Pro features along with Access Management for better management of a complex organizational architecture.

SOLICITATION # ITS-400335

d) *Explain the transportability and transferability of the proposed license agreements. Any licenses or warranties purchased on behalf of the State for this project must be transferable at the time the Vendor is paid under contract for said component*

DocuSign is a cloud SaaS solution and as such any licenses will be accessible from the time the order is processed between Carahsoft and DocuSign. North Carolina DIT sends a Purchase Order (PO) to Carahsoft and Carahsoft signs a DocuSign order form. Once the DocuSign order form is signed, the additional licenses or envelopes will appear in DIT's account. The licenses are easily transferred between users if needed as well.

3) *VIRTUALIZATION: Reserved*

N/A

4) *NCID: Reserved.*

N/A

5) *CLOUD SERVICE PROVIDERS (CSPs): For offers featuring a cloud-hosted solution, Vendors shall describe how the proposed solution will support the agency's information system security compliance requirements as described in the Statewide Information Security Manual, specifically relating to, and without limitation, the sections relating to cloud services: <http://it.nc.gov/statewide-resources/policies>. The e-Forms/e-Signature Program should be classified as NIST Moderate per the Statewide Information Security Manual and will be required to receive and securely manage data that is classified up to Restricted or Highly Restricted per the State's Data Classification and Handling Policy. To comply with policy, State agencies are required to perform annual security/risk assessments on their information systems using NIST 800-53 controls. This requirement additionally applies to all vendor provided, agency managed Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions. Assessment reports such as the Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, and ISO 27001 are preferred and offered solutions already meeting these requirements are requested to include these reports as part of their submission.*

Yes, DocuSign leads the industry with ISO 27001 PCI DSS, SSAE 16, Cloud Security Alliance (CSA) CloudTrust, and xDTM certified and tested internationally, across the entire company and its data centers. DocuSign has submitted these reports separately as part of our Security Trust and Assurance Packet (STAP) which was submitted via DocuSign on July 3 to Kristen Burnette.

DocuSign is FedRAMP Authorized - Moderate and is listed on the FedRAMP marketplace with a Government Community Cloud deployment model, <https://marketplace.fedramp.gov/index.html#/products>.

DocuSign's solution is ISO 27001:2013 certified and many of the ISO 27001:2013 controls are mapped to the NIST 800-53 requirements; we can provide additional information upon request.

DocuSign's top priority is the privacy and security of our customers' information, documents, and data. DocuSign meets or exceeds national and international security standards, including strict security policies and practices that set the standard for world-class information security.

- DocuSign delivers industry-leading data confidentiality with application-level AES 256-bit encryption, and our anti-tampering controls guarantee the integrity of customer documents, both in the process and completed
- We continually drive industry best practices in third-party audits and certifications, third-party assessments, and on-site customer reviews
- We're also the only eSignature company that provides unique features for non-repudiation, including digital audit trail and chain of custody

DocuSign's Certifications & Tests

DocuSign has Broadest Set of Security Certifications	
 <p>ISO 27001</p>	<ul style="list-style-type: none"> ✓ Global security gold standard: ISO/IEC 27001:2013 ✓ The highest level of global information security assurance available today ✓ Defines an information security management system (ISMS) ✓ Requires business continuity and disaster recovery plans that are tested regularly <p>DocuSign is the only eSignature service that is ISO 27001:2013 certified (renewed August 2017) to all 114 optional and mandatory ISO controls across the entire organization.</p>
 <p>SSAE 16 Type II Audit Completed</p>	<ul style="list-style-type: none"> ✓ Both SOC-1 Type 2 and SOC-2 Type 2 ✓ Security framework ✓ Controls testing ✓ Effectiveness measurements ✓ Service reliability <p>Provides assurance that DocuSign complies with the reporting requirements stipulated by the American Institute of Certified Public Accountants (AICPA). We undergo yearly audits across all aspects of our enterprise business and production operations, including data centers, and have sustained and surpassed all requirements.</p> <p>DocuSign is the only eSignature or DTM vendor auditor assured to both SSAE 16 SOC 1 Type 2 and AT 101 SOC 2 Type 2 auditor assured. Other vendors may claim auditor assurance to one of the SOC frameworks, but their scope may be limited. DocuSign recommends comparing the details of SOC 1 and SOC 2 auditor assurances to compare scope.</p>
 <p>FedRAMP <i>Authorized - Moderate</i></p>	<ul style="list-style-type: none"> ✓ A standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services <p>DocuSign received an Authorization to Operate (ATO) and is listed on the FedRAMP marketplace with a Government Community Cloud deployment model. To date, DocuSign is the only Digital Transaction Management (DTM) solution listed on the FedRAMP marketplace. Other vendors may claim FedRAMP authorization due to association with other company projects or data vendors, but a deeper examination of the FedRAMP Certification will showcase DocuSign's differentiation.</p>
 <p>xDTM CERTIFIED COMPANY</p>	<ul style="list-style-type: none"> ✓ The first standard of its kind to focus on Digital Transaction Management (DTM) ✓ Developed to raise the bar on quality and promote more trust and confidence in online business transactions ✓ Ensures that digital transactions are protected yet accessible—regardless of where parties reside or the devices used <p>DocuSign is the only DTM vendor certified compliant with the xDTM Standard, version 1.0</p>

SOLICITATION # ITS-400335

 <p>PARTICIPATING ORGANIZATION</p>	<ul style="list-style-type: none"> ✓ Data protection ✓ General computing controls focus ✓ Comprehensive scope (both as merchant and service provider), requiring third-party audits and the deepest level of examination ✓ Certified to PCI DSS 3.2 <p>As overseen by the Payment Card Industry Security Standards Council (PCI SSC), DocuSign places stringent controls around cardholder data as both a service provider and merchant. This compliance certifies safe and secure handling of credit card holder information.</p>
	<ul style="list-style-type: none"> ✓ Bestowed on cloud services that fully satisfy the most stringent requirements for data protection, identity verification, service security, business practices, and legal protection <p>This new certification demonstrates that DocuSign meets the highest CloudTrust rating possible as evaluated by Skyhigh Networks.</p>
	<p>Binding Corporate Rules</p> <p>DocuSign obtained approval of its applications for Binding Corporate Rules (BCR) as both a data processor and data controller from the European Union Data Protection Authorities. DocuSign's approved BCR enables lawful cross-border transfers of data through the DocuSign platform and eSignature service. As DocuSign implements these BCR, customers will be able to transact business with increased confidence knowing that they'll be complying with the upcoming GDPR data transfer requirements when using DocuSign. For more on DocuSign's BCR, visit GDPR and BCR on the Trust Center.</p>
	<p>The FISC develops security guidelines for information systems, which are followed by most financial institutions in Japan. These include guidelines for security measures to be put in place while creating system architectures, auditing of computer system controls, contingency planning, and developing security policies and procedures. Though compliance with the FISC Security Guidelines is not required by regulation nor audited by the FISC, DocuSign elected to become a member of the FISC and implemented internal controls to be compliant with the FISC Security Guidelines.</p>
<p><u>EU Trusted List</u></p>	<p>DocuSign is the only global cloud and mobile-ready digital signature solution with end-to-end workflows on this list of qualified trusted service providers. Please see the following for more information (https://www.ssi.gouv.fr/uploads/2016/07/tl-fr.pdf)</p>
<p><i>Compilation of (EU) Member States notification on SSCDs and QSCDs</i></p>	<p>This <u>publication</u> lists the signature devices that shall be considered as Qualified Signature Creation Devices (QSCDs) under the eIDAS regulation. DocuSign owns and operates a remote signature device which is listed in this publication and is the leading global eSignature solution offering cloud-based eIDAS-compliant electronic signatures.</p>

6) **BRANDING:** All offers that incorporate State design and branding, as specified by the State, shall adhere to the State style guide. The State style guide is located at: <http://digitalstyle.nc.gov>.

DocuSign is easily customizable and configurable. One method of customization is branding. Branding your DocuSign account is an excellent way to add the look and feel of the State's brand to the sending, signing, and email process – making it easier for users to identify envelopes coming from your organization. The DocuSign Account Custom Branding feature lets you set the colors, logo, and text for your account to enhance the sending and signing experience. You can create any number of

SOLICITATION # ITS-400335

brand profiles with different settings to reflect each of your different internal divisions or departments. Please note that when the State creates or changes a branding profile, it applies to everyone using that profile and affects all envelopes sent with that profile.

Emails can be customized with the State's logo and color scheme. The email subject line and email message can also be customized. A unique capability of DocuSign is that each recipient in a multi-recipient workflow can receive an individualized email, with different verbiage. In a multi-language scenario, each recipient may also receive a different, localized set of emails. Not only is the UI localized, but the email body is as well.

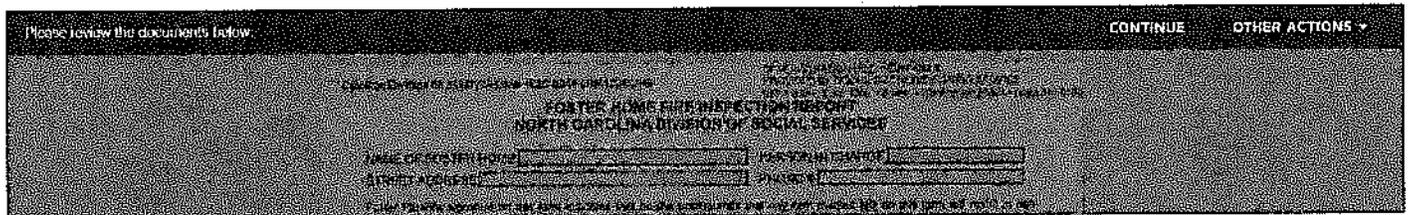
Organization Branding is Featured

The DocuSign branding appears in three (3) sections during signing – a “Powered by DocuSign” in the top right header, another “Powered by DocuSign” in the bottom left footer, and lastly, a “Copyright 2018 DocuSign” in the bottom right. Because DocuSign is recognized as the global standard of eSignature, this greatly assists the adoption rates for customers since a trust third party (DocuSign) is involved in the transaction. This is similar to the trust factor between banks, consumers, and the Visa logo that appears on a bank's credit card.

Please see the examples listed below of DocuSign's customization capabilities.

Please Review & Act on These Documents

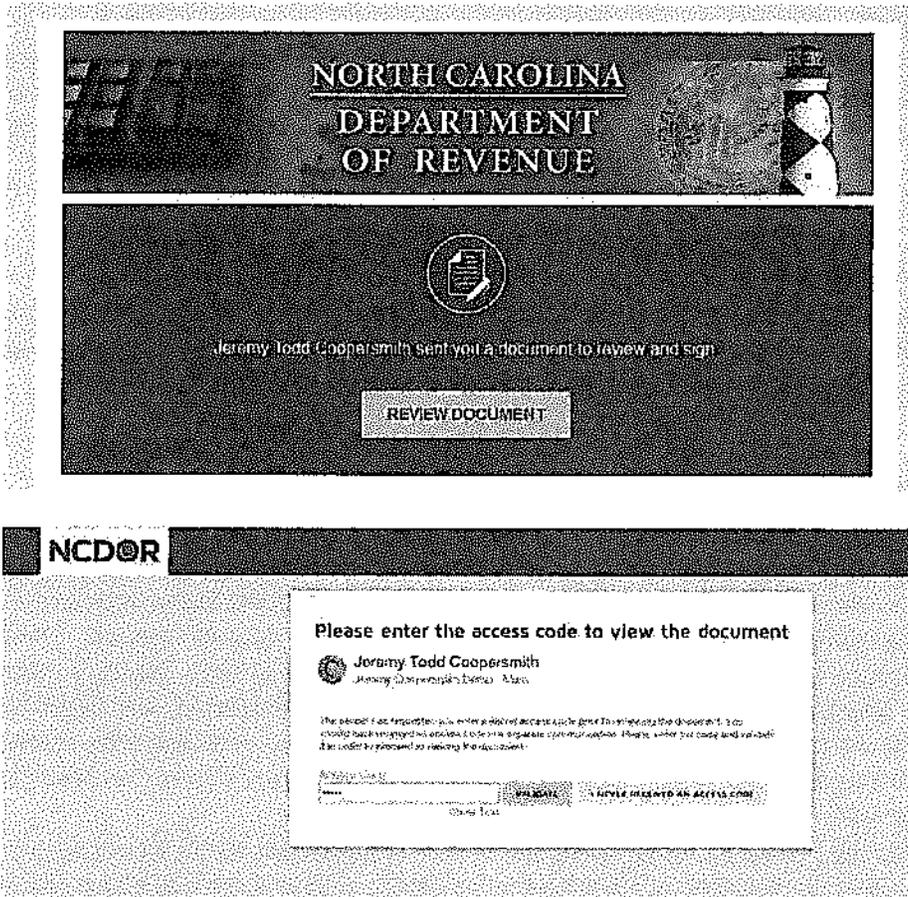
 **Jeremy Todd Coopersmith**
Jeremy.Coopersmith@ncs - Mail



Please Review & Act on These Documents

 **Jeremy Todd Coopersmith**
Jeremy.Coopersmith@ncs - Mail





7) **EQUIVALENT ITEMS:** Reserved.

Not applicable to DocuSign.

8) **LITERATURE:** All offers shall include specifications and technical literature sufficient to allow the State to determine that the proposed solution substantially meets all specifications. This technical literature will be the primary source for evaluation. If a specification is not addressed in the technical literature it must be supported by additional documentation and included with the offer. Offer responses without sufficient technical documentation may be rejected.

Acknowledged.

9) **EQUIVALENT GOODS:** Reserved.

Not applicable to DocuSign.

10) **DEVIATION FROM SPECIFICATIONS:** Any deviation from specifications indicated herein must be clearly identified as an exception and listed on a separate page labeled "Exceptions to Specification." Any deviations shall be explained in detail. The Vendor shall not construe this paragraph as inviting deviation or implying that any deviation will be acceptable. Offers of alternative or non-equivalent goods or services may be rejected if not found substantially conforming; and if offered, must be supported by independent documentary verification that the offer substantially conforms to the specified goods or services specification.

The E-Notary, Access Management and Organizational Administration features are only available with the DocuSign enterprise Pro, Enterprise Pro for Government, and Enterprise Pro for FedRAMP.

11) SCOPE OF WORK:

In 2013, the General Assembly transferred the responsibility of procuring electronic forms and digital signature services from the Office of the State Controller (OSC) to the Department of Information Technology (DIT) and the agency's State CIO. Thereby, per North Carolina State Legislation, the awarded solution must adhere to several technical requirements (Please see Section III, #12.)

Acknowledged.

12) TECHNICAL REQUIREMENTS:

In accordance with the legislative mandate, the awarded solution must conform with the following requirements. Vendors should read the information regarding each requirement and any corresponding reference, and provide detailed answers when prompted. Note: Solutions not adhering to technical requirements will not be considered by the State.

Acknowledged.

a) PII (Personal Identifiable Information)

N.C. Gen. Stat. §75-61(10) defines personal identifying information (PII), in part, as "[a] person's first name or first initial and last name in combination with identifying information as defined in G.S. 14-113.20(b)," and "identifying information" is defined by G.S. § 14-113.20(b) to include Social Security Number or employer taxpayer identification numbers, Driver's License, State Identification Card, or Passport Numbers, Checking Account Numbers, Savings Account Numbers, Credit Card Numbers, Debit Card Numbers, Personal Identification (PIN) Code as defined in G.S. § 14-113.8(6), Electronic identification numbers, electronic mail names or addresses, internet account numbers, or Internet identification names, Digital Signatures, any other numbers or information that can be used to access a person's financial resources, Biometric Data, Fingerprints, Passwords and Parents' legal surnames prior to marriage. Proposed solutions must adhere to PII protection laws. Therefore, please describe how the solution is PII compliant.

DocuSign is the global standard for electronic signature and System of Agreement (SofA). Our intuitive product is protected by unmatched security and offers the strongest levels of legal enforceability in eSignature, including a non-repudiation audit trail, carrier-grade encryption, tamper-proof certificates, a chain of custody, and multi-factor authentication.

All envelope and encrypted data is keyed to the customer account and sending account identity using unique identifiers. Access to data is restricted to the owning account by the application and is logically isolated. All documents and other sensitive customer data are stored in an encrypted fashion in a secure datacenter which is physically segregated from DocuSign's corporate networks. DocuSign's key escrow ensures that no internal DocuSign personnel or third parties can view customer documentation.

DocuSign employs Opportunistic TLS, meaning that we will connect with the newest version of TLS supported by both sides of the connection. Some customers use older servers, workstations, and browsers which do not support TLS 1.2 and therefore we will try and establish a connection with them using TLS 1.1 or 1.0 in that order. DocuSign will not establish a connection using any version of SSL. Data in transit is encrypted using TLS 1.2 with 256-bit keys on HTTPS secured web pages and at rest using AES encryption with 256-bit keys.

Additionally, DocuSign has completed a Privacy Impact Analysis (PIA) as part of the DocuSign's FedRAMP authorization.

b) HIPAA (Health Insurance Portability and Accountability Act)

The Contractor agrees that, if the Division determines that some or all of the activities within the scope of this contract are subject to the Health Insurance Portability and Accountability Act of 1996, P.L. 104-91, as amended ("HIPAA"), or its implementing regulations, it will comply with the HIPAA requirements and will execute such agreements and practices as the Division may require to ensure compliance. HIPAA forms, instructions and other materials can be located on the HIPAA web site: <http://hipaa.dhhs.state.nc.us/index.html>. If applicable, proposed solutions must adhere to HIPAA laws. In consideration of this requirement, please describe how the proposed solution is HIPAA compliant. Please note that the State requires a business associates agreement (BAA).

Yes, DocuSign is HIPAA compliant as a Business Associate.

Due to the encryption configuration and security controls associated with the DocuSign Signature services, DocuSign personnel will not have access to or know the nature of PHI contained within our customer's documents within the envelopes. Our customers are in sole control of the types of documents and data uploaded to the account.

If applicable, customers are responsible for (i) implementing appropriate privacy and security safeguards to protect their PHI in compliance with HIPAA and (ii) using the available controls within the services to support their HIPAA compliance requirements. There is no HIPAA certification for a cloud provider such as DocuSign, however, DocuSign uses reasonable and appropriate safeguards to prevent unauthorized use or disclosure of our customer's PHI that they may place into our system, as evidenced by DocuSign's ISO 27001 certification, SSAE 18 audits, and other third-party attestations and certifications.

c) PCI (Payment Card Industry)

The Payment Card Industry (PCI) Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents. In consideration of this requirement, please describe how the proposed solution is PCI compliant.

The Payment Card Industry Data Security Standard (PCI-DSS) is a set of information security requirements that any entity touching credit card data must comply with, as mandated by the major credit card brands. As an organization that is both a service provider and a merchant, DocuSign undergoes annual audits by a Qualified Security Assessor that validates our compliance from both perspectives.

The following information is contained in our Security Packet on PCI-DSS compliance:

Attestation of Compliance (AOC) – Service Provider

A service provider as defined by PCI is "a business entity that is not a payments brand, directly involved in the processing, storage, or transmission of card holder data on behalf of another entity." This document attests to DocuSign's compliance with the current version of the PCI-DSS as a service provider.

Attestation of Compliance (AOC) – Merchant

A merchant as defined by PCI is "any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, Mastercard, or Visa) as payment for goods and/or services." This document attests to DocuSign's compliance with the current version of the PCI-DSS as a merchant with an eCommerce payment channel.

DocuSign & Client PCI Responsibilities Matrix

This document is provided in order to assist our Customers in meeting of PCI-DSS Requirement 12.8.5, "Maintain information about which PCI-DSS requirements are managed by each service provider and which are managed by the entity."

d) FERPA (Family Educational Rights & Privacy Act)

The Family Educational Rights & Privacy Act (FERPA) states that student educational records are subject to 20 U.S.C. 1232g, Family Rights and Privacy Act (FERPA). Therefore, the Vendor must ensure that the proposed solution fully complies with FERPA and every employee responsible for carrying out the terms of this contract is aware of the confidentiality requirements of federal law. In addition, every such employee must sign a confidentiality acknowledgement that indicates that he or she understands the legal requirements for confidentiality. The Vendor is responsible for the actions of its employee and must take all precautions necessary to ensure that no violations occur. Finally, access to personally identifiable student education information shall be limited to those employees who must have access to it in order to perform their responsibilities pursuant to this contract.

In compliance with the law, please describe the following:

- 1. Describe the capabilities of tracking and reporting the application access.*

All aspects of each transaction are fully logged (including name, email address, IP address, date/time, authentication, and activity) and captured in a detailed transaction history which is stored in perpetuity as hashed and encrypted data within the DocuSign system. This data is available on demand from the DocuSign system and may also be programmatically exported to client systems in real-time as transactions progress to a completed state. In addition, DocuSign also generates a Certificate of Completion for every transaction in the form of a digitally signed PDF document which is designed to be a court admissible document.

Audit trails, such as signatures and documents, are always stored in encrypted form using an x.509 certificate. A hash is also taken before each change, and compared to previous SHA-2 hash values to ensure the document has not been modified. After any change, a new hash is taken and stored physically and logically separate from the document.

DocuSign tracks activities at both a User and Transaction (Envelope) level. This is relevant both to an auditing perspective as well as driving the workflows around the document being signed. All the audit activities listed below are available to the Sending party through the user interface or programmatic API.

From the standpoint of a Signing User, DocuSign audits the following events:

- When a User was invited to sign, including whether the invitation was successfully delivered
- When a User passed (or failed) various authentication steps that were required to access the documents
- When a User agreed to a Consumer Disclosure consent
- When a User first viewed the documents
- When a User signed their documents
- Anytime a User downloaded the documents
- Anytime a User viewed the documents
- When a User declines to sign the documents
- Anytime a User marks-up a document or provides data values

From the standpoint of the Sender, DocuSign audits the following events:

- When the sender initiated the Envelope
- When the sender activated the Envelope for signature
- Anytime the sender modifies the Envelope contents or signature workflow
- Anytime the sender downloads the documents
- Anytime the sender views the documents
- When a sender voids the Envelope (revoke the ability to eSign)

From the standpoint of a Transaction: DocuSign audits the following events:

- When the Envelope was initiated
- When the Envelope was activated for signature

SOLICITATION # ITS-400335

- When the Envelope was viewed by all parties
- When the Envelope was signed by all parties
- When the Envelope was completed
- When the Documents were deleted
- When the physical location of the electronic Envelope was transferred to another electronic vault

Additionally, audit logs include changes to Permission Sets. Changes captured include:

- New permission set
- Edited permission set
- Deleted permission set

2. Describe the solution's approach to handling non-public data at rest and non-public data in motion.

Data in transit is encrypted using TLS 1.2 with 256-bit keys on HTTPS secured web pages and at rest using AES encryption with 256-bit keys.

3. Describe the solution's approach for encrypting data such that only the intended recipient can decrypt it.

All envelope and encrypted data is keyed to the customer account and sending account identity using unique identifiers. Access to data is restricted to the owning account by the application and is logically isolated. All documents and other sensitive customer data are stored in an encrypted fashion in a secure datacenter which is physically segregated from DocuSign's corporate networks. DocuSign's key escrow ensures that no internal DocuSign personnel or third parties can view customer documentation.

4. Describe the solution's process for handling and notification of a breach of non-public data.

DocuSign maintains an ISO 27001, PCI-DSS, SSAE18, and FedRAMP examined and tested Incident Response Program and Notification policies and processes. All incidents are to be reported via a standard internal form to ensure consistency of information capture. The full policies are restricted and are not shared outside of our offices.

DocuSign's InfoSec team retains the list of customers requiring specific notification within specific timeframes. Upon detection of any customer information within DocuSign's control that may have been improperly accessed or acquired by an unauthorized party, DocuSign references the data accessed to determine the type of exposure, the population of customers impacted, and the nature of the acquiring individual or entity.

DocuSign maintains a data breach notification program to promptly notify customers in the event their information is lost or experiences unauthorized access. DocuSign will promptly notify customers in the event that their protected data is reasonably believed to be lost or stolen in an unencrypted format, or subject to unauthorized access by, or is used or disclosed as a result of an authorized acquisition. DocuSign will provide notice in writing promptly after discovery of such a security incident, but in no event later than the deadline set forth under applicable Law or the applicable business agreement, whichever is earlier.

To the extent this information is not known when the initial written notice is first provided, DocuSign will promptly supplement this written notice, in writing when information becomes known (unless specifically directed otherwise by a law enforcement organization). Please note: these notifications are not automatic.

5. For authorization, describe the solution's handling of various roles associated with data access.

DocuSign maintains formal policies and procedures including our DocuSign Access Control policy. DocuSign's employee logical access authorization chain required direct manager approval, application/ data source owner approval, and cases of sensitive applications and data sources, security management approval. Access to critical applications and data sources is

SOLICITATION # ITS-400335

removed at employee termination and is reviewed at least quarterly to verify that appropriate and current access levels are maintained.

DocuSign enforces the rule of least privilege and has documented segregation of duties. DocuSign enforces formal logical and account separation of the development, quality assurance (QA), and production environments.

From a customer point of view, DocuSign customers have an administrator of their own that controls who has specific levels of access. They do user management, including adding and closing users, as well as determining the permissions of those users.

e) Security

The state potentially handles a large amount of non-public data. Proposed solutions must adhere to North Carolina Statewide IT Security Policies and Standards (<https://it.nc.gov/statewide-information-security-policies>), as they may relate to personal and/or confidential data. Therefore, please address the following:

The State also requires that all systems connected to the State network or process State data, meet an acceptable level of security compliance. This includes those systems that operate outside of the States' direct control such as Cloud Services defined as Software as a Service (SaaS), Infrastructure as a Service (IaaS) or Platform as a Service (PaaS). Attachment B provides a high-level view of specific security requirements that are requirements to meet compliance. Vendors must fill out the VENDOR ASSESSMENT GUIDE in Attachment B.

Note: There may be additional requirements depending on the sensitivity of the data and other Federal and State mandates.

The following items are security and/or solution requirements; therefore, describe how the solution will accommodate the following:

1. *The solution must alert the user to any changes to a document after a digital signature has been applied.*

DocuSign adheres to the ISO 32000-1 technical specification for Portable Document Format (PDF) and EN 319 411 technical specification for digital signatures. By following these technical specifications, most PDF readers (e.g. Adobe, Foxit, etc.) automatically validate the digital signatures embedded in PDF documents downloaded from DocuSign. If a document has been tampered after being downloaded from DocuSign, the PDF reader displays a warning message to the user.

2. *The digital signature service component must require users to prove their identity before applying an electronic signature to a document.*

DocuSign provides multiple authentication options.

* Email Address: Requires access to a specific email address before access is granted.

* Access Code: Requires the signer to provide a sender-generated code shared out of band, usually over the phone. The signer must enter the code to open the document.

* SMS: A two-factor solution that requires the signer to provide a randomly-generated one-time passcode sent via SMS text message to the signer's mobile phone to open the document.

* Federated Identity/Single Sign-On: Federated Identity. Validates authentication by an external system integrated with DocuSign via the industry-standard protocol SAML.

* Third-party: Validates the signer's Salesforce, Google, Yahoo!, or Microsoft account credentials, with additional options for social network credentials from Facebook, Twitter and LinkedIn.

* DocuSign Credentials: Validates a recipient's existing DocuSign account associated with a username and password.

* ID Check: This third-party service by LexisNexis validates a signer using a KBA (knowledge-based authentication) process. The signer must correctly answer a list of personally identifying questions to open the document (OFAC Checking and Age Verification can be part of this).

SOLICITATION # ITS-400335

* Two-Factor Phone Authentication: This third-party service from Authentify by Early Warning validates a signer's access to a phone number and predetermined access code for entry. The signer's spoken name is also recorded as a biometric print.

*STAN PIN System: Validates the person's Student Authentication Network as entered.

*Digital Certificate: DocuSign offers digital certificates as part of its Standards-Based Signatures platform. Using digital certificates during signing provides higher levels of identity authentication and document transaction security. Further explanation of DocuSign's Standards Based Signatures can be found here:

<https://www.docusign.com/sites/default/files/standards-based-digital-signatures.pdf>

Signer Authentication Methods

Email Address	Access Code	3 rd Party Web ID	In-person Signing
→ DocuSign Account	SMS Access Code	Social ID	ID Check / KBA
Federated / SSO	Phone Call	Digital Certificate	Electronic Notary
Google ID	Facebook ID	Yahoo ID	MSFT ID

3. *The solution must provide digital certificates to establish non-reputation (i.e. cannot deny receipt or signature).*

Yes, with DocuSign's digital signatures (X.509 standard certificate backed signatures). DocuSign has the breadth and depth of digital signatures capabilities far beyond any other vendor. Other solutions have a high-friction solution for signers, and in many cases their solution is incapable of functional implementation. DocuSign has completed three acquisitions and spent two years in product development to bring a unique digital signature solution to market called Standards-Based Signatures. DocuSign's Standards-Based Signatures can enable hundreds of digital signature use-cases that no other vendor's solution can support. Specifically, DocuSign's Standards-Based Signatures offer the following unique differentiators.

- i. Mobile digital signatures – sign with a digital certificate from DocuSign's native mobile app. DocuSign is the only vendor that enables signers to easily complete a digital signature transaction with low friction from a mobile phone.
- ii. End-to-End cloud digital signatures – senders can select which type of certificate a signer must use to sign from the cloud, and a signer can sign using that certificate all within the cloud for a low-friction, completely seamless experience.
- iii. DocuSign doesn't require desktop software for digital signatures (unless specifically required by certain 3rd party certificate authorities). DocuSign was the first solution that can complete an end-to-end digital signature transaction in the cloud without downloading a document to the desktop, installing desktop software, or installing special web plug-ins.
- iv. DocuSign can issues digital certificates as a certificate authority
- v. DocuSign has on-premises digital signature options with the industry's leading digital signature hardware, the DocuSign Signature Appliance (DSA). The DSA's most advanced on-premises digital signature and certificate management capabilities.
- vi. DocuSign also offers the DocuSign Hybrid Cloud to meet digital signature on-premises cloud digital signature requirements

4. *The solution must provide digital hashes to establish fixity (i.e. guarantees that digital documents have not been altered since completion).*

DocuSign adheres to the EN 319 411 technical specification which describes the process to calculate the document hash within the digital signature. Further, this technical specification details encrypting the hash with the private key from the X.509 certificate. In addition, this technical specification explains the process to embed the encrypted hash and X.509 certificate into the Document Security Store (DSS) within the PDF file. By following this technical specification, DocuSign establishes fixity for the document hash.

C. RESPONSE TO TECHNICAL SPECIFICATIONS

1. General Features

Provide the general features of the proposed solution. Please include the following information:

a. *Use this prompt to articulate an understanding of the state's need as well as any value-added services relevant to this RFP.*

DocuSign is an electronic signature and workflow management application hosted in a datacenter. Customers determine and manage the documents and workflow used in their instance of DocuSign. DocuSign enables customers to directly upload documents for signature over secure sessions where the customer documents are systematically encrypted. DocuSign personnel do not have access to customer documents/data.

System of Agreement (SofA) is category of cloud services designed to digitally manage document-based transactions. SofA removes the friction inherent in transactions that involved people, documents, and data to create faster, easier, more convenient, and secure processes.

Our platform moves beyond the electronic signature solution. With the electronic signature solution, you can easily sign and send documents for electronic signature within minutes. DocuSign's solution moves beyond that feature and focuses on the digital execution of business transactions. The SofA solution focuses on combining nine major elements:

1. **Automation/Workflow** - Automates and controls transaction processes. This includes workflow that can be configured by a business user.
 2. **Assembly** - Manages the creation, assembly and delivery of data and documents into and out of key applications and processes.
 3. **E-Signatures** - Enables parties to securely sign a document.
 4. **Agreement Collection and Management** - Supports collection of digital agreements.
 5. **Identity** - Provides identify proofing for all participants.
 6. **Application and Services Integration** - Integrates key applications and cloud based document sources.
 7. **Secure Transaction** - Provides a centralized secure transaction center.
 8. **Audit History** - Full, tamper-proof audit trail of transaction that meets evidentiary standards and is admissible in court proceedings.
 9. **Enterprise Administration & Control** - Enables enterprise provisioning, permissioning, management, and reporting.
- DocuSign's Workflow Management is designed to support the complexity of global organizational processes. Senders can simplify a sophisticated signing and reviewing process by using drag and drop routing that allows for complete flexibility. Signers and Reviewers are assigned different roles and levels of document visibility, which can also be amended while the document is in flight by using DocuSign Correct. The Correct feature is unique and allows for control plus flexibility.

DocuSign is the global standard for electronic signature and System of Agreement (SofA). Employees at all the Fortune 100 and many other large enterprises in nearly every country in the world have used DocuSign. Our intuitive product is protected by unmatched security and supported by world-class customer service, a rich partner ecosystem, and an unbeatable track record of system uptime results. DocuSign also offers the strongest levels of legal enforceability in eSignature, including non-repudiation audit trail, carrier-grade encryption, tamper-proof certificates, chain of custody, and multi-factor authentication. In fact, it's more legally enforceable than paper and pen. DocuSign is ISO 27001 certified as an information security management system (ISMS).

b. *Address the solution's capacity to include ad hoc workflow routing rules, based on unique business rules defined for document(s) and signature requirements.*

DocuSign provides the ability to route document(s) with simple and complex workflows that can incorporate multiple signers and group signing in a combination of serial and parallel workflows. These workflows can be placed on a transaction (document(s)) within a pre-defined template or an ad hoc document send. A user of the system can manage the workflow based on their level of access to change the templates for ongoing workflow management. If using the ad hoc sending of a document, the sender can manage the workflow settings.

c. *Can the solution deliver business process workflow for documents, from originator to signatories?*

Yes. DocuSign supports serial, parallel and mixed routing workflow(s) across DocuSign's web application, Nits mobile applications, and within integrations such as DocuSign for Salesforce. DocuSign allows you to put powerful workflow creation tools in the hands of your business users.

- Route documents to your recipients in any order (e.g. serial, parallel, or mixed)
- Assign recipient-specific tasks including signing, viewing or copy receipt
- Utilize predefined documents, data and workflow, and route to signers and other recipients
- Enable signer self-service and list-based sending with PowerForms and Bulk Sending

d. *Can the solution integrate with global address books or pull users into a centralized address book?*

Yes. DocuSign includes a Contacts list to help make sending documents even easier. When you send a document, the recipients are automatically added to your Contacts list. You can use the Contacts list to quickly add recipients to the documents you send.

Contacts sharing an email address

- The State can have contacts who share a single email address, such as a husband and wife, or business partners sharing a company email
- The State can add both contacts to a document and each recipient receives an email notification at the shared email address
- The State can add, modify, and delete entries in your Contacts list through the My Preferences > Account view

Please note: Your personal contacts list is optimized for up to 500 contacts. While you can have more than 500 contacts saved, for performance reasons, you can only scroll through the first 500. To locate contacts beyond the first 500, you can use the Search function.

e. *Address whether the solution will permit external party signing, including two-factor or multi-factor authentication. Provide examples.*

DocuSign supports both serial and parallel workflow, and a combination of the two, with an unlimited number of recipients. Both internal and external signers are supported, *in any order*. Senders can view a graphical representation of the workflow by selecting the 'Order Diagram' link within each template and envelope.

In addition to the Signer Authentication Methods mentioned above, DocuSign offers several Sender Authentication Methods.

Sender Authentication Methods

DocuSign Account	Federated / SSO	Two-Factor (SMS & Phone)
---------------------	-----------------	-----------------------------

DocuSign's authentication methods:

- Increase legal enforceability
- Ensures the highest level of data privacy
- Meets authentication regulations and best practices (e.g. FFIEC and CSA recommendations)
- Supports access control requirements for security certifications, including ISO 27001

f. Describe the capability to establish evidentiary requirements for signed documents.

DocuSign Audit History is a full, tamper-proof audit trail of each transaction that meets evidentiary standards and is admissible in court proceedings. This is exportable as a Certificate of Completion that confirms the validity of your transactions. DocuSign warrants full compliance of our documents and audit trails with the federal E-SIGN Act.

All aspects of each transaction are fully logged (including name, email address, IP address, date/time, authentication, and activity) and captured in a detailed transaction history which is stored in perpetuity as hashed and encrypted data within the DocuSign system. This data is available on demand from the DocuSign system and may also be programmatically exported to client systems in real-time as transactions progress to a completed state. In addition, DocuSign also generates a Certificate of Completion for every transaction in the form of a digitally signed PDF document which is designed to be a court admissible document.

Audit trails, such as signatures and documents, are always stored in encrypted form using an x.509 certificate. A hash is also taken before each change, and compared to previous SHA-2 hash values to ensure the document has not been modified.

After any change, a new hash is taken and stored physically and logically separate from the document.

DocuSign tracks activities at both a User and Transaction (Envelope) level. This is relevant both to an auditing perspective as well as driving the workflows around the document being signed. All the audit activities listed below are available to the Sending party through the user interface or programmatic API.

From the standpoint of a Signing User, DocuSign audits the following events:

- When a User was invited to sign, including whether the invitation was successfully delivered
- When a User passed (or failed) various authentication steps that were required to access the documents
- When a User agreed to a Consumer Disclosure consent
- When a User first viewed the documents
- When a User signed their documents
- Anytime a User downloaded the documents
- Anytime a User viewed the documents
- When a User declines to sign the documents
- Anytime a User marks-up a document or provides data values

From the standpoint of the Sender, DocuSign audits the following events:

- When the sender initiated the Envelope
- When the sender activated the Envelope for signature

SOLICITATION # ITS-400335

- Anytime the sender modifies the Envelope contents or signature workflow
- Anytime the sender downloads the documents
- Anytime the sender views the documents
- When a sender voids the Envelope (revoke the ability to eSign)

From the standpoint of a Transaction: DocuSign audits the following events:

- When the Envelope was initiated
- When the Envelope was activated for signature
- When the Envelope was viewed by all parties
- When the Envelope was signed by all parties
- When the Envelope was completed
- When the Documents were deleted
- When the physical location of the electronic Envelope was transferred to another electronic vault

Additionally, audit logs include changes to Permission Sets. Changes captured include:

- New permission set
- Edited permission set
- Deleted permission set

g. Describe the process of creating new forms and templates.

DocuSign's templating capabilities allow the State to standardize and manage repeatable processes across your organization. This is typically done and managed by a business user – there is no coding or archaic naming conventions. It is accomplished via a simple, drag-and-drop user interface.

Templates help streamline the sending process when you frequently send the same or similar documents. Templates allow you to create a standard document, with set recipient roles, signing tags and information fields. Templates can also contain the signing instructions for the document and any signature attachments.

When there are some differences in the information needed for a document, a sender can still use a template to provide some recipient and tag information, while still allowing the sender to make additions and changes to the document before sending.

- Utilize predefined documents, data and workflow, and route to signers and other recipients
- Automatically apply tags and workflow based on previously sent documents with Intelligent Template Recognition (ITR)
- Distribute and restrict template access to individual, pre-defined groups or company-wide
- Easy to set up—no coding required
- Enable signer self-service with PowerForms

With DocuSign templates, the State can:

- Quickly and easily send documents
- Avoid inaccurate data, incorrect workflow or incomplete documents
- Automatically enforce even the most complex approval workflows

DocuSign templates offer significant, differentiating capabilities when compared to other vendors "templates". For example:

SOLICITATION # ITS-400335

Unlike other signature providers, DocuSign does not require the original document to be edited to include textual markers which designate locations for signature, dropdown, radio buttons, etc. DocuSign provides multiple methods to a pre-determined location:

1. Drag/Drop, with SAVE.as an electronic form...without modifying the underlying document
2. Use of naturally occurring text. For example, "Sign Here:" might already be within the document (or "In Witness thereof"). A DocuSign signature or field may be specified to automatically occur in a position relative to the text (move down xxx and to the right xxx, whenever you find yyy)
3. Use a textual marker overtly included within the document. Other vendors provide this, but DocuSign additionally allows you to specify what the textual clue should be.
4. Allow the signer to decide

h. Address whether each person in the workflow is given the opportunity to review all documents, with confirmation opportunity, before the transaction continues.

Yes, in a serial workflow, DocuSign gives all recipients the opportunity to review the documentation before the transaction proceeds.

i. The State needs the signing process to be simple, and require very few steps for users. The steps required to secure signatures should not become more burdensome for any staff involved than current paper processes. Therefore, describe if the solution configures predefined workflow routing rules based on specific business rules defined for document(s) and signature requirements.

DocuSign is intuitive and easy to use. A step by step process showing how to sign a document is included below.

When someone sends you a DocuSign document for your electronic signature, you first receive an email from DocuSign sent on behalf of the sender.

Step 1 Review the DocuSign email

Open the email and review the message from the sender. Click **REVIEW DOCUMENT** to begin the signing process.

Note: Your experience as a signer may also vary depending on how the document sender wants you to sign. New signers have a different experience than returning signers and signers with a DocuSign account. To learn more, watch the Signing video or read the how-to guide Signing Documents Electronically with DocuSign.

Step 2 Agree to sign electronically

Review the consumer disclosure, and select the checkbox I agree to use Electronic Records and Signatures. Click **CONTINUE** to begin the signing process.

Important! To view and sign the documents, you must agree to conduct business electronically.

Note: To view additional options, click **OTHER ACTIONS**. For more information of other actions available, please review our Signing Documentation.

Step 3 Start the signing process

1. Click the **START** tag on the left to begin the signing process. You are taken to the first tag requiring your action.

2. Click the **SIGN** tag. You are asked to Adopt Your Signature.

Step 4 Verify your name

Verify that your name and initials are correct. If not, change them as needed.

Step 5 Adopt a signature

Do **one** of the following:

- Accept the default signature and initial style, and go to the next step.
- Click **CHANGE STYLE**, and select a different signature option.
- Click **DRAW**. Draw your signature/initials using a mouse, or your finger or a stylus on a touchscreen.

Step 6 Save your signature

Click **ADOPT AND SIGN** to adopt and save your signature information and return to the document.

Step 7 Confirm signing

When you finish clicking all signature tags in the document, confirm signing by clicking **FINISH**.

A message appears stating that you have completed your document. You can now download a PDF copy or print a copy of the document. The sender receives an email with the signed document attached, and the signed document appears in their DocuSign account.

- j. Describe the solution's capacity to store completed, digitally signed document(s), on the State's own Document Management System; Include whether the:
- Solution supports grouping and/or compartmentalization of originators (i.e. by department, function, division, section) so that documents may not be visible to disparate workgroups.
 - Originators monitor the progress and status of transactions they and/or their workgroups have initiated.

Storage

All the State's transactions are securely stored in the cloud with DocuSign. You can also access and store completed documents to Box, Dropbox, OneDrive, Google Drive, Evernote, and Salesforce. All transactions are stored in our service indefinitely unless a customer chooses to set a retention policy and are accessible from the account that initiated the transaction. With DocuSign, there are no storage size limitations.

Compartmentalization

Yes – viewer permissions can be set by group. The User Group management option allows administrators to create user groups, assign users to the groups, and set the user permissions for the groups. You are not required to set Permission Profiles for a group, but this makes it easier to manage user permissions for a large number of users without having to change permissions on a user-by-user basis. Groups can also be used with template sharing to limit user access to templates. There are two default groups in the system: Everyone and Administrators. Other groups with customized permissions can easily be added to suite your needs.

Monitor Status

DocuSign makes viewing the status of transactions simple and intuitive. Throughout the signing process, DocuSign tracks and displays the status of all participants and documents in the process.

Every envelope that you create or receive through DocuSign, has a status. The status indicates the current state of the transaction. This list defines all the possible statuses:

- **Draft:** For an envelope, you created and then saved without sending. Draft envelopes now show the creation date when viewing the envelope details.
- **Sent:** The email notification has been sent to at least one recipient. The envelope remains in this state until all recipients have viewed the document. (Shown in Reports and History only)
- **Delivered:** All recipients have viewed the document. (Shown in Reports and History only)

SOLICITATION # ITS-400335

- **Waiting for Others:** The envelope has at least one recipient who has yet to complete their action. The recipient status in the Details view shows whether the outstanding recipients need to sign (Needs to Sign) or view (Needs to View). From the Manage page, you can see whose turn it is to sign by hovering over the status.
- **Needs to Sign:** You are a recipient and you need to sign.
- **Needs to View:** You are a certified delivery recipient and you are required to view the document.
- **Correcting:** The sender started to correct an in-process envelope and has not yet saved his changes. In this state, any outstanding signers are unable to view or sign. The sender must either save or cancel his changes to move the envelope out of the Correcting status.
- **Voided:** The sender canceled the envelope before it was completed. Recipients can no longer view or sign the document. Voided documents appear in your sending account as voided. You can still view and print the document, though it has a "VOID" watermark.
- **Declined:** A signer has declined to sign.
- **Completed:** An envelope is completed once all the recipients have completed their actions.
- **Expired:** A document that has exceeded its set expiration period without completing will expire. Recipients can no longer view or sign the expired document. Expired documents appear in your sending account as voided. You can still view and print the document, though it has a "VOID" watermark.
- **Delivery Failure:** The email notification did not reach the recipient. Review the Details to see which recipient status is listed as 'Auto Responded.' For this recipient, check the email address you entered and correct the document to fix any errors. From the 'Manage' page, you can see which recipient delivery failed by hovering over the status warning.

k. Describe if the solution facilitates digital signing of documents via a computer web browser with modern browsers. Specify minimum software versions supported.

DocuSign is an on-demand SaaS (Software as a Service) platform. Aside from an HTML5 web browser, which is standard on most mainstream browsers, for signing and a PDF reader to optionally view documents which may be exported from DocuSign, there are no additional software requirements.

DocuSign supports the following browsers: Latest stable release (except where noted) of Internet Explorer® (11.0 or above); Windows Edge; Mozilla® Firefox®; Safari™; Google Chrome®.

In general, no browser plug-ins, extensions, or add-ons are required. For the latest requirements: <https://support.docusign.com/guides/ndse-user-guide-system-requirements>

However, if a State Agency has an X.509 certificate on a smart card on their PC, then they will need to have Java running on their PCs and will install our Standards Based Signature (SBS) plug-in.

l. Describe if the solution facilitates digital signing of documents on IOS, Android, and Windows smart phones. Specify minimum software versions supported.

DocuSign does support digital signatures on mobile devices. The SBS feature enables users to leverage DocuSign's cloud-based Express and Protect & Sign offerings to issue certificates on-the-fly and digitally sign documents. Additionally, the SBS enables customers to deploy DocuSign Signing Appliances within their data centers to store certificates and digitally sign documents within the standard Signing experience on the SaaS platform. No additional software is required for these mobile digital signature options.

m. Also include whether the solution facilitates digital signing of documents on IOS, Android, and Windows mobile tablet devices. Specify minimum software versions supported.

DocuSign does support digital signatures on mobile devices. The SBS feature enables users to leverage DocuSign's cloud-based Express and Protect & Sign offerings to issue certificates on-the-fly and digitally sign documents. Additionally, the SBS enables customers to deploy DocuSign Signing Appliances within their data centers to store certificates and digitally sign documents within the standard Signing experience on the SaaS platform. No additional software is required for these mobile digital signature options.

n. Address if the solution can create and manage multiple levels of system access.

DocuSign allows for a deployment that consists of a Parent Account/Child Account hierarchy to separate key organization users for privacy reasons. Furthermore, DocuSign delivers industry-unique capabilities to manage enterprise deployments at an organization level with full control over visibility and permissions of users at both an organizational and sub-account level. Users can be assigned to multiple accounts, but State administrators have a global view and control over what permissions, groups, and documents those users have access. DocuSign is the only product in the market that offers this type of organizational administration. Our most recent organizational administration offers:

- Streamline and simplify the process of managing users and permissions across your organization.
- View all your accounts from a centralized location
- Keep your organization's information secure with domain-level user administration.
- Self-service setup and manage your Organization for identity management
- Identify which corporate users have external accounts.
- Define the default account for your domain users to route envelope traffic where you need it to go.
- Administer just-in-time provisioning configurations
- Manage your Organization's administrative team

Organization administrators can automatically activate user memberships – removing the requirement for users to activate their accounts via email. This is applicable for domain users on accounts linked to the State. This is especially important for embedded workflow scenarios or when the signer must have an active account membership.

Additionally, we have included a white paper with best practices building policies and Standard Operating Procedures for a comprehensive System of Agreement framework. Please see **OTHER SUPPORTING MATERIAL INCLUDING TECHNICAL SYSTEM DOCUMENTATION** for more information.

o. Describe if the solution will provide a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that: (1) the electronic document was not altered without detection during transmission or at any time after receipt; (2) any alterations to the electronic document during transmission or after receipt are fully documented.

Yes - through DocuSign's multi-faceted verification of signing events, customers can rely on the authenticity of signers. DocuSign provides unique features for non-repudiation, including digital audit trail and chain of custody. DocuSign provides a digital audit trail for the customer to track signing and lifetime access events. A formal Certificate of Completion is created upon signature of all document parties.

Documents exported from DocuSign are digitally signed for tamper evidence. The tamper seal is an X.509 PKI standards based "Digital Signature" that is applied to the document at the time it is downloaded from DocuSign. The mechanism would indicate if the document has been changed since being downloaded. DocuSign provides a digital audit trail for the customer to

track signing and lifetime access events. This Certificate of Completion is also tamper sealed upon download. This is so the Certificate of Completion cannot be modified after download, just like the document.

p. Clarify that the solution disallows any form of unauthorized copying or pasting signatures.

DocuSign does not permit copying and pasting of signatures to a document. If a user tries to copy or paste a signature to a document downloaded from DocuSign, the additional image changes the document hash. When opening an altered PDF document, the PDF reader (e.g. Adobe, Foxit, etc.) displays a warning message because the new document hash doesn't match the document hash embedded as part of the digital signature.

q. Describe if the solution will determine if any modifications were made after the signature for the relevant sections were attached and disallow modifications or invalidate corresponding section that was modified.

Documents completed using the DocuSign Signature service come embedded with the digitized signature, a unique Envelope ID, and a certificate of completion that describes relevant transaction data (date signed, IP address of signer, method of signing, timestamps, method of authentication, etc.) related to the document (transaction). DocuSign embeds other meta data into the downloaded version which enables tamper-free validation. Further, DocuSign maintains a certificate of completion and makes available to the sender and all nominated recipients a copy of the completed document signed using the DocuSign Signature service.

In both cases it is up to the viewer of the document to validate that the tamper seal is still intact.

r. Explain if the solution will contain the copy of record, which will include

- *All electronic signatures contained in or logically associated with that document.*
- *The date and time of receipt.*
- *Any other information used to record the meaning of the document or the circumstances of its receipt.*
- *Other, such as authorized system ID of signature owner, authorized computer ID, smart device ID such as MAC address, location data, etc.*
- *Detection of unauthorized data modification and place obvious marker on the document – electronic version and paper version.*
- *A function to alert users of needed actions.*

All aspects of each transaction are fully logged (including name, email address, IP address, date/time, authentication, and activity) and captured in a detailed transaction history which is stored in perpetuity as hashed and encrypted data within the DocuSign system. This data is available on demand from the DocuSign system and may also be programmatically exported to client systems in real-time as transactions progress to a completed state. In addition, DocuSign also generates a Certificate of Completion for every transaction in the form of a digitally signed PDF document which is designed to be a court admissible document.

Documents exported from DocuSign are digitally signed for tamper evidence. The tamper seal is an X.509 PKI standards based "Digital Signature" that is applied to the document at the time it is downloaded from DocuSign. The mechanism would indicate if the document has been changed since being downloaded. DocuSign provides a digital audit trail for the customer to track signing and lifetime access events. This Certificate of Completion is also tamper sealed upon download. This is so the Certificate of Completion cannot be modified after download, just like the document.

2. Product Strategy Roadmap

The state needs a fully-developed plan Provide a 12-month Vendor product strategy as it relates to the solution proposed.

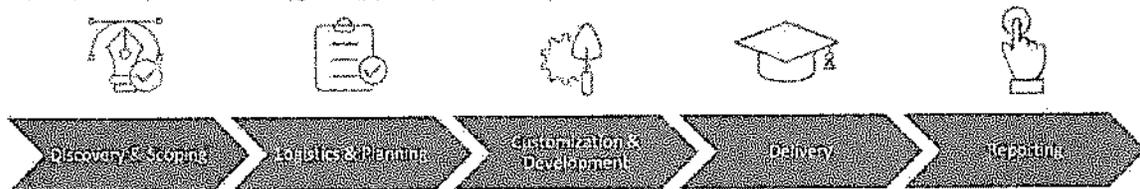
In addition to the customized 12-month Program that we developed specifically for the State of NC which follows these sections, we have multiple training offerings available.

Training Services

DocuSign offers a broad set of training programs to meet your individual needs.	
Rapid Adoption Program (Onboarding)	All Rapid Adoption Program participants will go through DocuSign's standard customer onboarding process and materials and will have access to DocuSign University's self-paced learning paths on product functionality via the DocuSign Learning Portal in the first 90 days. Additional training is offered by DocuSign's Learning and Enablement team.
FastStart Implementations - Train-the-Trainer	All FastStart implementations include one DocuSign Administrator Train-the-Trainer session (up to 2 hours) covering the new deployment and account administration for a maximum of five users (if necessary). Includes DocuSign's standard Train-the-Trainer materials consisting of a presentation based on the Configuration Workbook that's delivered during the project closeout process which can be used by the customer to conduct end user training. The DocuSign API FastStart will also include an additional one-hour overview training on DocuSign APIs that's focused on the customer's particular integration solution.
Custom Engagements	For larger custom engagements and deployments, learning and enablement services are often bundled into statements of work or sold separately post-implementation to support a customer's deployment or learning strategy. Below is a high-level overview of DocuSign's Learning and Enablement capabilities: <ul style="list-style-type: none"> • Self-paced Learning • Virtual Instructor-led Workshops • Custom End User Training • Admin Courses • Custom Videos • Enterprise Enablement Packages
DocuSign University (DSU)	The DocuSign University Learning Portal provides DocuSign users with access to an extensive catalog of self-paced and instructor-led courses to help build knowledge and expand expertise. To support an organization's learning needs, courses are available for a wide range of DocuSign roles and in multiple languages to learn DocuSign anywhere, anytime. See Learning & Enablement section for a complete portfolio of services.

Training Approach

Below is a visual illustration of DocuSign's approach to how we develop a and deliver an Enterprise Enablement Program.



Support & Self-Service Resources

Resolve issues faster to accelerate your business

DocuSign Customer Support gives you the ability to choose the right level of ongoing assistance you need to get the value you expect from our platform. Our industry-leading global support model is there to back you up, no matter where you are or how you want to engage – whether it's on the web, via online case management, live chat, phone or our team of dedicated technical support professionals on-hand 24x7, who know your solution inside and out.

Customer Support Operating Hours & Languages

General Customer Support

There are many ways (phone, chat, email or web communities and knowledge base) for customers and employees who are wishing to escalate customer issues to contact Customer Support depending on what service-level package the customer has purchased or the urgency of an issue.

Operating Hours

Support Levels	Free	Plus	Premier	Enterprise
Contact Method (Channel)	Online Case Chat Phone	Online Case Chat Phone Click-to-Call	Online Case Chat Phone Click-to-Call Email	Online Case Chat Phone Click-to-Call Email
Hours of availability*	24/7 7 days a week	Sun: 2:30 – 11 PM PT Mon - Thurs: 24/7 Fri: 12 AM – 8 PM PT	Sun: 2:30 – 11 PM PT Mon - Thurs: 24/7 Fri: 12 AM – 8 PM PT	Sun: 2:30 – 11 PM PT Mon - Thurs: 24/7 Fri: 12 AM – 8 PM PT

DocuSign Support Center

The **DocuSign Support Center**, <https://support.docusign.com/>, is a free resource which provides a comprehensive library of reference documents and videos which take you step-by-step through the process. DocuSign's Support Center also includes a Case Management dashboard for logged in users.

Other Self-Service Support Resources

You'll also benefit from on-demand access to an extensive digital library of self-service resources including an active support community, an extensive knowledge base, product video tutorials and current release notes. At the end of the day, we strive to maintain a high standard of service and expert advice which results in a growing community of satisfied customers.

- **DocuSign Support Community**, <https://support.docusign.com/forum>, – an online forum where you can access help, ask questions, and collaborate with other DocuSigners. Community Moderators review posts to make sure they are helpful and appropriate.
- **Knowledge Market**, <https://support.docusign.com/en/knowledgemarket> – provides tools and tips on how to drive adoption of DocuSign. Some of the available resources are white papers, value studies, videos, and tools.

- **DocuSign University Learning Portal**, <https://support.docusign.com/en/docusignuniversity> - a self-service learning tool utilized by customers throughout their DocuSign journey – beginning with your onboarding experience all the way to becoming a DocuSign expert. Users can browse self-paced learning paths and curated courses by role and type, as well as have access to DocuSign's entire training catalog.

State of North Carolina's 12-month Plan

A training and activity plan has been developed specifically for the State. This plan will help agencies, who are new to DocuSign, learn about the service and become trained in best practices. This will reduce DIT's effort in bringing on new agencies to the service and will also allow agencies to be self-sufficient and adopt DocuSign for maximum effectiveness.

Based on our experience with thousands of implementations, we found that there are three main types of users:

- Administrators
- Senders & Template Builders
- Signers

The flexible training plan is organized by these three types of users and is a combination of self-paced courses (on-demand training) and live, Instructor-led workshops. These training courses are included in our proposal and are *no charge* to DIT or the participating agencies, thus adding additional value to the State.

Create a personalized, flexible plan for your learning.

Search the Training Catalog on the DocuSign University Learning Portal to choose courses and workshops with topics that matter for you.

Training Catalog

Managing Envelopes as a Sender

Categories

- ▣ Languages
- ▣ English



Search by Title
Filter by Course Type
Choose your Language
Explore by Role



How Long?

Self-Paced Courses: 10-60 min.
Workshops: 90-min.

ADMINISTRATORS

Getting Started

- Configuring Your DocuSign Account Settings
- Branding a DocuSign Account
- Managing Users on Your DocuSign Account
- Understanding Why and How to Establish Custom Permission Sets
- Understanding Why and How to Establish User Groups
- Using User Management Features for Groups and Users

Advanced Concepts

- Understanding Admin Integrations
- Standard and Customized Reporting for Admins
- Understanding Basic Template Creation

SENDERS & TEMPLATE BUILDERS

Getting Started

- Getting Started with Sending Envelopes
- Overview of Basic Signing, Sending and Envelope Management
- Managing Envelopes as a Sender
- Template Basics
- Getting Started with Templates
- Sending an Envelope with a Template
- Using Additional Recipient Actions When Sending
- Using Document Fields
- Using Reporting as a Sender

Advanced Concepts

- Creating Advanced Text Fields Using Validation, Specific Formatting and Collaboration
- Using Advanced Fields and Actions When Sending
- Creating Template with Multiple Documents and Recipients
- Sending to Bulk Recipients
- Creating a PowerForm from a Template
- Using PowerForms as a Sender

SIGNERS

Getting Started

- Getting Started with Signing Envelopes
- Overview of Basic Signing, Sending and Envelope Management
- Managing Envelopes as a DocuSign Signer

Advanced Concepts

- Using Advanced Features When Signing Envelopes
- Recognizing Authentication Methods for Signers

KEY  = Self-paced  = Live, Instructor-led workshop

Questions? DocuSignUniversity@DocuSign.com

ADMINISTRATORS

<p>MONTH 1</p> <p>Overview of Basic Signing, Sending, and Envelopes Management</p> <p>Configuring Your DocuSign Account Settings</p>	<p>MONTH 2</p> <p>Creating a DocuSign Account</p> <p>Managing Users on Your DocuSign Account</p>	<p>MONTH 3</p> <p>Using User Management Features: Invitations and More</p> <p>Understanding Why and How to Establish Custom Permission Sets</p> <p>Understanding Why and How to Establish User Groups</p>
<p>MONTH 4</p> <p>Configuring Recipient Signing Settings</p> <p>Configuring Document Signing Settings</p> <p>Configuring Recipient Sending Settings</p>	<p>MONTH 5</p> <p>Understanding Basic Envelope Creation</p> <p>Sharing Envelopes Between Users</p>	<p>MONTH 6</p> <p>Understanding Recipient Authentication and Account Security Settings</p>
<p>MONTH 7</p> <p>Standard and Customized Reporting for Admins</p>	<p>MONTH 8</p> <p>Understanding Admin Integrations</p>	<p>MONTH 9</p> <p>Bulk Send</p> <p>Sending to Bulk Recipients</p>
<p>MONTH 10</p> <p>Creating a Powerform from a Template</p> <p>Using Powerforms as a Sender</p>	<p>MONTH 11</p> <p>Managing Your Envelopes</p>	<p>MONTH 12</p> <p>DocuSign Digital Transformation Project Manager Fundamentals</p>

KEY  = Self-paced  = Live, Instructor-led workshop

SENDERS & TEMPLATE BUILDERS

<p>MONTH 1</p> <p>Overview of Basic Signing, Sending and Envelope Management</p> <p>Getting Started with Sending Envelopes</p>	<p>MONTH 2</p> <p>Using Additional Recipient Actions When Sending</p> <p>Using Document Fields</p> <p>Using Reporting as a Sender</p>	<p>MONTH 3</p> <p>Managing Envelopes as a Sender</p> <p>Understanding Basic Template Creation</p>
<p>MONTH 4</p> <p>Template Basics</p> <p>Getting Started with Templates</p> <p>Sending an Envelope with a Template</p>	<p>MONTH 5</p> <p>Managing Your Envelopes</p> <p>Understanding Recipient Authentication and Account Security Settings</p>	<p>MONTH 6</p> <p>Sharing Envelopes Between Users</p>
<p>MONTH 7</p> <p>Creating Advanced Text Fields Using Validation, Specific Formatting and Collaboration</p> <p>Using Advanced Fields and Actions When Sending</p>	<p>MONTH 8</p> <p>Creating Templates with Multiple Documents and Recipients</p>	<p>MONTH 9</p> <p>Bulk Send</p> <p>Sending to Bulk Recipients</p>
<p>MONTH 10</p> <p>Creating a PowerForm from a Template</p> <p>Using PowerForms as a Sender</p>	<p>MONTH 11</p> <p>Managing Your Envelopes</p>	<p>MONTH 12</p> <p>Managing your Templates</p>

KEY  = Self-paced  = Live, Instructor-led workshop

SIGNERS

<p>MONTH 1</p> <p>Overview of Basic Signing, Sending, and Envelope Management</p> <p>Getting Started with Signing Envelopes</p>	<p>MONTH 2</p> <p>Managing Envelopes as a DocuSign Signer</p> <p>Using Advanced Features When Signing Envelopes</p>	<p>MONTH 3</p> <p>Recognizing Authentication Methods for Signers</p>
<p>MONTH 4</p>	<p>MONTH 5</p>	<p>MONTH 6</p>
<p>MONTH 7</p>	<p>MONTH 8</p>	<p>MONTH 9</p>
<p>MONTH 10</p>	<p>MONTH 11</p>	<p>MONTH 12</p>

KEY  = Self-paced  = Live, Instructor-led workshop

DocuSign Account Team Activities



<p>MONTH 1</p> <p>Lunch and Learn Hosted in Raleigh</p>	<p>MONTH 2</p> <p>Online Webinar on "The Art of the Possible"</p>	<p>MONTH 3</p> <p>QBR with NC DIT</p> <p>Solution Day</p>
<p>MONTH 4</p>	<p>MONTH 5</p> <p>Online Webinar on "The Art of the Possible"</p>	<p>MONTH 6</p> <p>QBR with NC DIT</p>
<p>MONTH 7</p> <p>Lunch and Learn Hosted in Raleigh</p>	<p>MONTH 8</p> <p>Online Webinar on "The Art of the Possible"</p>	<p>MONTH 9</p> <p>QBR with NC DIT</p> <p>Solution Day</p>
<p>MONTH 10</p>	<p>MONTH 11</p> <p>Online Webinar on "The Art of the Possible"</p>	<p>MONTH 12</p> <p>QBR with NC DIT</p>

3. Disaster Recovery and Hosting Facilities

The state needs to understand the hosting facilities, capabilities and disaster recovery capabilities of the proposed solution, and requires an application disaster recovery plan as well. In addition to these needs, please address the following:

a. Explain how the vendor will work with the state to develop this plan and integrate it with agency operation.

Business Continuity Planning and Enterprise Disaster Recovery:

DocuSign performs Business Continuity testing on an annual basis that DocuSign determines is appropriate for their environment. This testing involves the following:

- Failover of selected DocuSign systems.
- Information Security Tabletop exercises
- Companywide communication testing
- Pandemic Testing
- DERT:
 - Emergency response team exercises completed throughout the year
- First Aid/CPR,
- Physical safety and security
- Emergency response team drills fire drills,
- Companywide personal safety and awareness training.

With DocuSign's carrier-grade architecture, secure replication is performed in near real-time to our geo-diverse active systems. DocuSign designs all deployments to be fully redundant and fault tolerant. There are no single points of failure in our load balanced, redundant configuration. Our environment uses load balancers to spread load throughout multiple servers. If a server fails or experiences an issue it should be transparent to users using our system. In addition to SQL clustering and server load-balancing we also have redundant networking gear that replicates customer documents up to 9 times across the systems that can recover in the event of a failure of any. All data is replicated at the OLTP level and all historical and document data is synchronized using a proprietary document replication service. The system is constructed to offer a worst case 5-minute recover point objective in the event of a single site catastrophic failure.

Since data is replicated to geographically dispersed data centers traditional backups are unnecessary, while DocuSign does make 8 perpetual backups of blob data, along with weekly full and daily differential backups of the database as well as maintaining 5 active nodes. In the event of a disaster or total site failure in any of the active systems, all user activity is served by the remaining. DocuSign's failover capability is tested monthly during monthly site maintenance.

DocuSign's datacenters are commercial-grade, PCI DSS compliant, and SSAE 16 examined and tested. DocuSign's carrier-grade Architecture features three simultaneously active & redundant systems that allow the overall system to survive full site outages so it's "always on". Customer data is stored up to nine times across the three geographically disparate locations. RTO = 15 mins RPO = 5 min

b. The data that is stored in this application's database may be confidential and if so, must follow HIPAA, FERPA, PII and PCI compliance. Explain how the vendor will protect this data in the case of an event that requires execution of the disaster recovery plan.

Please see our response above which explains how data is replicated to geographically dispersed datacenters; thus traditional backups aren't necessary. Our data protection remains the same.

c. Describe the hosting facilities. Use diagrams where appropriate. Consider the following aspects:

- *Who is the hosting provider? Where is the primary site? Where is the disaster recovery site?*

DocuSign Federal is hosted in four (4) co-location datacenter facilities within the continental United States specifically chosen due to their adherence to industry-standard physical security and availability protections. These datacenter facilities are

SOLICITATION # ITS-400335

located in Chicago, Illinois; Seattle, Washington; and Richardson, Texas. The facilities are managed by Cyxtera (Chicago and Seattle), SunGard (Richardson), and Equinix (Chicago) and meet common industry security control requirements, including SSAE16 and FISMA controls. DocuSign Federal is housed within heavily access-restricted datacenter cages within each facility, with multiple layers of physical access control, authentication, and authorization before personnel or information system components are permitted access. Further, DocuSign Federal has dedicated multi-tenant security appliances and network area storage units to segregate Federal Agency data from other DocuSign customers. In addition to the datacenter facilities, certain ancillary DocuSign Federal components are hosted within AWS, Azure, and Akamai. These components are logically integrated with the network boundary present in the datacenter facilities.

- *Explain if the hosting facilities are SAS 70 II compliant and/or compliant with SSAE 16 reporting standards, please provide copies of the most recent audit(s).*

Yes, please see the DocuSign Security Trust and Assurance Packet.

- *What is the data center's classification (Tier 1, Tier 2 etc.)?*

Tier 3

- *What policies are in place to thwart insider breaches?*

DocuSign uses a McAfee ELM to capture logs from DocuSign Federal production components. The McAfee SIEM produces alerts based off of the logs from the ELM. Houston, an in-house DocuSign tool, forwards those alerts to the Redmine ISCM to automatically generate cases to be analyzed by the CSIRT team, to ensure the system components are functioning in an optimal, resilient, and secure state.

CSIRT monitors the automatically generated ISCM cases for unauthorized access to and use of DocuSign Federal in accordance with AU-2.

CSIRT uses a SIEM solution to capture and correlate all application logs from system components and tools within DocuSign Federal. All Windows and CentOS servers send system event logs to the SIEM. Additionally, FIM (OSSEC), ClamAV, SCEP, and SNORT IDS forward system event logs to the SIEM.

DocuSign has also built an in-house performance monitoring solution, KazMon, which deploys local custom agents to monitor performance and events related to the system components and web applications within DocuSign Federal. These logs are not forwarded to the SIEM, but are centrally managed via the in-house built KazMon solution. Additionally, KazMon monitors for any changes against the baseline OS configurations.

The SIEM uses the ELM to manage logs in a read-only mode and retain logs for one (1) year. DocuSign limits access to the SIEM, ELM, and audit infrastructure to authorized CSIRT and Information Security members, in accordance to AC and IA control families, to protect the information obtained during monitoring.

CSIRT heightens monitoring activities as necessary due to vulnerabilities or suspicious activities are uncovered within DocuSign Federal. In addition, CSIRT heightens monitoring activities when there are alerts from external sources which includes Technical Security Alerts and Security Bulletins from US-CERT as well advisories from FedRAMP. CSIRT can create dashboards or other visualizations in the SIEM to track specific events, specific platforms, or combinations thereof. DocuSign obtains legal opinions with regard to monitoring as necessary. In accordance with AC-8, DocuSign notifies all users accessing DocuSign Federal about monitoring. Further, DocuSign obtains users' consent of such monitoring as a requirement in order to access the system.

SOLICITATION # ITS-400335

For events that meet the pattern of a known attack methodology, CSIRT track and document validated security incidents as new cases within ISCM. CSIRT follows the Incident Response Playbook to resolve the incident and notifies the applicable DocuSign Federal stakeholders as needed.

• *What is the process for background checks? Who are they performed by, for which employees, are the checks performed at employment, yearly, etc.*

DocuSign conducts criminal background check investigations. Criminal background reports are a factor in determining whether an offer of employment will be extended, and criminal background verification is essential prior to any offer being provided to an individual.

Background Checks

Criminal Background Checks

DocuSign conducts criminal background check investigations. Criminal background reports are a factor in determining whether an offer of employment will be extended, and criminal background verification is essential prior to any offer being provided to an individual.

Employment Verification

DocuSign conducts prior employment verification of all personnel as part of the hiring process. This process also includes professional reference checks of previous managers and colleagues. Employment verification is a factor in determining whether an offer of employment will be extended or withdrawn.

Additional Checks

Additional content for all prospective DocuSign employees:

a. Social Security Number verification

b. Multi-State Criminal Database search:

i. Using the candidate's name and date of birth, Sterling Talent Solutions searches case, sentencing, disposition, and other criminal-related records for all available jurisdictions in the United States.

c. Nationwide Sex Offender Registry:

i. Sterling Talent Solutions searches for the candidate in the sex offender registries of all 50 states, the District of Columbia, and Puerto Rico.

d. County Criminal Record Verification (10-Year Address History):

i. The 10-Year County History Search is a live search of real-time county criminal records based on the applicant's address history. An SSN trace is conducted to verify the individual's identity, to identify any aliases that should be searched, and to produce an address history for the individual. Sterling Talent Solutions dispatches online research teams to search for real-time information in all jurisdictions where the individual has lived for the past 10 years.

• *Will all customer data be housed within the continental United States?*

Yes. Customers may select the country for the datacenter space, either U.S., EU, Canada, or Australia. If the US is selected, then yes, the data will be stored in the U.S. U.S. DocuSign has ten data centers in geographically distinct locations in United States, European Union, Canada, and Australia. DocuSign currently has three (3) interconnected data centers in the United States, three (3) interconnected data centers in the European Union, two (2) interconnected data centers in Canada, and two (2) interconnected data centers in Australia. DocuSign is a leader in providing your choice of data center storage.

• *Are there any circumstances when the solution would store customer data and intellectual property outside of the United States or with a non-USA owned institute?*

Please see our previous response.

4. Data Management

a. *Describe how data is archived and/or purged.*

DocuSign provides options for the storage and purging of data. Data and/or document(s) can be stored in DocuSign without limitation of space. Organizations may decide to use the cloud storage for all of their data or certain parts. The data/document(s) will stay securely in DocuSign under your specific retention policies. All data/documents are securely housed under your specific security access rules. These allow you to determine who can/cannot see it in the system.

If desired, you are able to enforce auto-purge rules to delete the data/document(s) from the system. This will provide the ability to enforce data retention policies. After the desired timeframe, all respective data/document(s) will be placed into a two week hold before the full purge. This allows for the ability to reverse a purge if necessary (or if done in error). As a part of the transactions in DocuSign and certificate of completion is created to include the necessary audit history and non-repudiation details. This documentation is not purged from the system as this is important for you to always be able to gain access to the most important legally-binding details if ever needed.

b. *The State must receive an attestation letter explaining how the Vendor destroyed the data when the State separates from the Vendor. Please acknowledge that the solution will supply such communication.*

DocuSign customers determine their account's retention policies. Once a document/envelope is deleted, it is also deleted on a near real-time basis from the three active sites. If a customer ceases services, they have 90 days to retrieve their documents. In addition, customers are free to purge those documents at any time and can use the API to verify that it has been completed.

All aspects of each transaction are fully logged (including name, email address, IP address, date/time, authentication, and activity) and captured in a detailed transaction history which is stored in perpetuity as hashed and encrypted data within the DocuSign system. This data is available on demand from the DocuSign system and may also be programmatically exported to client systems in real-time as transactions progress to completed state. In addition, DocuSign also generates a Certificate of Completion for every transaction in the form of a digitally signed PDF document which is designed to be a court admissible document.

c. *Describe how the state will get its data back in a form that can be used. What costs will be involved if any?*

As the data/documentation is important to be able to retrieve from the system, DocuSign provides multiple options for its retrieval, whether manual or automated. These include:

1. **Manual Download:** Upon the completion of a transaction (or at any time during the routing), a User with access to the transaction can manually download the document(s), audit history, Certificate of Completion, and Field Data (in CSV format). This is a typical process when integrations are being designed/built. DocuSign also informs each and every person in the routing order of the transaction completion and can provide them with the ability to download the document(s) as well as the Certificate of Completion.
2. **Connect Push:** As a part of the subscription to DocuSign, you are provided with Connect. This is an automated push that can be set up to send data/document(s) to a posted URL for parsing by a listener. This allows for the push of the information to a central location that can be taken and sent to any and all internal systems for storage and/or triggering of additional workflow steps/processes.
3. **API Call/Integration:** Open WebServices APIs in REST and SOAP are provided for the connection of internal systems to DocuSign. You can set up connections to initiate transactions as well as to retrieve the completed data/document(s), etc. Many organizations utilize these API capabilities to pull the data/document(s) into internal systems to create objects, update records, and/or store the data/document(s) electronically for future retrieval.

SOLICITATION # ITS-400335

4. Retrieve: This is a separate application that is used for specific scenarios that are typically based on certain searching or eDiscovery needs. This is a windows-based application that can search for specific characteristics within the transactions. This application does have an additional cost.

- d. *How is the data destroyed at the end of a term contract?*
• *Address how workflows, meta-data and configurations will be transferred to the state.*

The State of North Carolina owns its own data and documents. DocuSign does not have access to the data. Data and documents can be provided to the state via bulk export.

5. Audit

The state retains the right to audit the physical environment (could apply to production, secondary site, etc.) where the vendor application/service is hosted per the vendor proposal. Therefore, describe what processes the solution has in place to allow this audit?

- a. *Describe if the solution will provide a retrievable audit trail.*

Every transaction that is processed via DocuSign will automatically create a full audit history as well as a Certificate of Completion that contains all of the non-repudiation details. Obtaining this information can be done via:

1. Manual Download:
 - a. Audit trail (in DocuSign) can be retrieved from the transaction itself. This includes all steps completed in the process along with transaction ID details, and (if applicable) the geo location of the activities.
 - b. Certificate of Completion can also be retrieved directly from the transaction in DocuSign console/mobile app. This document is presented in a tamper-evident PDF.
2. Email communication:
 - a. Certificate of completion can be attached to the completion emails sent from the system upon completion of a transaction.
3. Automated Pull/Push:
 - a. API integration can be used to pull any data, document(s), transaction details, and audit history from the system to place in other desired system(s).
 - b. DocuSign "Connect" can be used to push any and all data/document(s) to a posted URL to be pulled and parsed by an internal listener.

- b. *Supply the chain of custody for obtaining the record of copy.*

DocuSign Users can obtain the appropriate document(s)/record(s) from the system based on their respective visibility restrictions. There are also options around sharing of transactions within the system as well as tiered-level visibility to provide the visibility across Users.

Anyone who is in a routing order for a transaction can be provided with the documentation (and Certificate of Completion) via email notification.

- c. *Address if the solution can export capabilities for the audit trail data. List possible export formats.*

Audit Trail data/documents can be pushed/pulled from the system via "Connect" or API integration. This is typically presented in XML format.

SOLICITATION # ITS-400335

d. Describe if audit event details are available to customer in a reusable format (i.e. CSV, Excel, PDF).

Audit Trail data can be retrieved in PDF from the record. Is an integration is used, data can be pulled in XML format for further use.

e. Describe how the Audit trail is stored and secured against tampering.

Within DocuSign, the audit history is housed within each transaction respectively. This information cannot be tampered with in the system.

Upon receiving the data within the Certificate of Completion, it is presented as a tamper-evident sealed PDF. This document is always sealed with an X509-backed digital certificate to ensure the validity of the document.

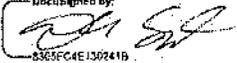
f. The solution must track every event in the signature process. Therefore, describe to what degree such details and events are being stored.

Every step in the routing order is tracked from viewing steps to signature actions. Below is an example of the detailed tracking that is done within the transaction:

Envelope History				
6/28/2018 10:43:17 pm	Jeremy Todd Coopersmith (English (US)) [web:107.77.201.233]	Registered	The envelope was created by Jeremy Todd Coopersmith	Created
6/28/2018 10:43:22 pm	John Smith (English (US)) [web:107.77.201.233]	Opened	John Smith opened the envelope [documents:(Amusements Registration Application (Fillable Form)_0.pdf)]	Sent
6/28/2018 10:43:26 pm	John Smith (English (US)) [web:107.77.201.233]	Viewed In- Session	John Smith viewed the envelope in a session hosted by Jeremy Coopersmith Demo - Main [documents: (Amusements Registration Application (Fillable Form)_0.pdf)]	Sent
6/28/2018 10:47:04 pm	John Smith (English (US)) [web:107.77.201.233]	Payment Authorized	John Smith authorized payment by Credit Card	Sent
6/28/2018 10:47:07 pm	John Smith (English (US)) [web:107.77.201.233]	Signed	John Smith signed the envelope	Sent

g. Explain how consent from users to use the service is tracked as an auditable action.

It is up to the organization how they want to enforce the agreement to sign electronically. You can make that a requirement upon every time someone interacts with a DocuSign process step or have it so that they only have to accept the first time that they interact from that email address. This agreement is tracked within the transaction certificate of completion as seen below:

Signer Events	Signature	Timestamp
<p>John Smith jicsigner+JS@gmail.com Treasurer, Board of Directors ABC Company Security Level: Email, Account Authentication (None), Authentication</p> <p>Authentication Details SMS Auth: Transaction: 25912023D43412049041A961A24A7652 Result: passed Vendor ID: TeleSign Type: SMSAuth Performed: 6/28/2018 1:15:45 PM Phone: +1 610-413-5304</p> <div style="border: 1px solid black; padding: 2px;"> <p>Electronic Record and Signature Disclosure: Accepted: 6/28/2018 1:17:35 PM ID: b9fc9ce2-0ff0-4c52-a994-7b22bd0f8c63</p> </div>	<p>DocuSigned by:  8365FC4E130241B</p> <p>Signature Adoption: Drawn on Device Using IP Address: 107.77.201.233 Signed using mobile</p>	<p>Sent: 6/28/2018 12:57:12 PM Viewed: 6/28/2018 1:17:35 PM Signed: 6/28/2018 1:18:48 PM</p>

6. NCID

For Identity Management, the state has invested in a common solution called NCID. NCID is the State's enterprise identity management (IDM) service and is operated by the North Carolina Office of Information Technology Services. (The details of NCID can be found at: <https://it.nc.gov/ncid/>.) Additional information regarding this service can be found in the ITS Service Catalog at: <http://www.its.state.nc.us/ServiceCatalog/Index.asp> (see Identity Management - NC Identity Management under the main menu item Application Services).

In consideration of this environment, describe the solution's capabilities to integrate with NCID. Also, explain the solution's capability to externalize NCID. Within Section IV, Cost Proposal, include an estimate to integrate NCID with the proposed solution understanding that this is a decentralized solution and will be invoiced by the individual agencies.

Please also address the following:

- a. *Describe how the solution handles varying roles for authorization. Such as guest account (citizen non-authenticated), administrators, etc.*

Access to DocuSign is managed centrally by your system Administrator(s) and is therefore fully controlled with options of integrating into SSO for on-time provisioning.

Any 'User' of DocuSign can access the transactions that they have responsibilities in via the web console and/or mobile app. If desired, Users can also be forced to log in every time they click on the link to sign a document from an email notification.

For non-Users ("Signers"), DocuSign provides the ability to authenticate based on the following options:

1. Email: Signer are automatically communicated to via email with a link to get to the document(s) for signing. This provides a single level of authentication into the respective email. There are times when a secondary email authentication is needed (ex: PowerForm self-service model initiated from a link on a website) where DocuSign will send an email to the Signer's email account with a pin code to enter into the transaction.
2. Access Code: A pin code can be set per Signer that requires successful entry into the transaction to get to the document(s) for signing.
3. SMS Text: A pin code can be sent to the Signer's mobile phone to allow them to enter for access to the document(s) for signing.
4. Phone: A phone call can be placed to a Signer's phone to accept a verbal agreement to us electronic signatures. This records the Signer stated their name for the acceptance to sign electronically.

SOLICITATION # ITS-400335

5. Knowledge-based: Through an integration with LexisNexis, you can require that a Signer successfully pass a series of questions about themselves to gain access to the document(s) for signature. You can set the option to allow for multiple chances at this as well.

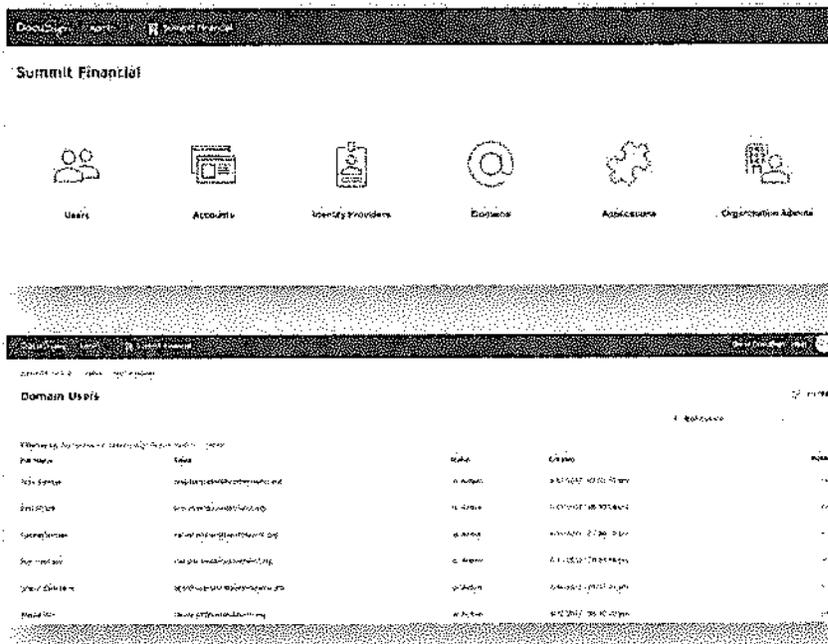
All authentication procedures can be used in conjunction with each other for multi-factor needs. All details around the authentication are stored in DocuSign transaction history and provided within the Certificate of Completion as a part of the non-repudiation details.

Information is included below on our Organization Administration feature, but as we mentioned in our Executive Summary, we have new features that will be released in the next few months. We are unable to include roadmap capabilities in our proposal response, but we are happy to provide a demonstration of our upcoming release capabilities in a presentation.



Organization Administration

A new DocuSign infrastructure that empowers you to better control and manage how DocuSign is used by your organization.



Organizations often require multiple DocuSign accounts to protect the security of account data, meet the unique needs of specific accounts, accommodate different billing systems, or comply with regulations where the account data should physically reside. Managing multiple accounts is challenging and time consuming. DocuSign admins strive to efficiently manage and control all their DocuSign accounts and users in a consistent, compliant and secure manner.

Organization Administration centralizes all DocuSign accounts and users managed by you into a single location.

- Gain confidence in how DocuSign is being used at your organization through centralized visibility and management.
- Keep your organization's information secure with domain-level user administration.
- Streamline and simplify the process of managing users and permissions across your organization.



Features

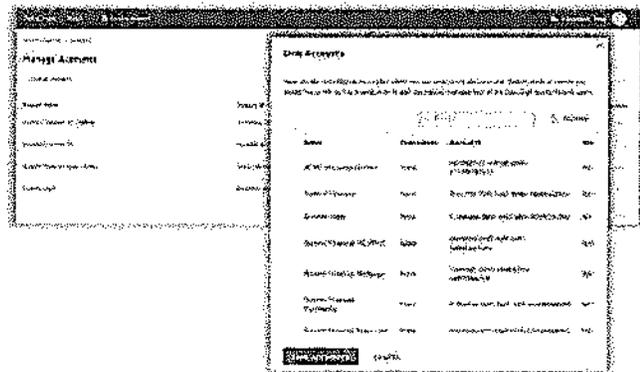
Centralized User Management

- Set up your Organization to view all accounts in a single location
- Create and directly manage users from the Organization
- Assign and modify account memberships for a user from the user profile card
- Gain visibility of all paid and freemium accounts that were created using your organization's email domain(s)
- Manage your Organization's administrative team
- Control a user's default account for signing and sending



Self-Service Identity Management

- Self-service setup and configure Single Sign-On (SSO)
- Administer just-in-time user provisioning
- Change a user's email address



About DocuSign

DocuSign is changing how business gets done by simplifying anyone to send, sign and manage documents anytime, anywhere, on any device with trust and confidence. DocuSign and On to keep life and business moving forward.

For U.S. Inquiries: toll free 866 219 4319 | DocuSign.com

For EMEA Inquiries: phone +44 203 714 4800 | email: emea@docuSign.com | docuSign.co.uk

For APAC Inquiries: phone +61 2 9392 1998 | email: apac@docuSign.com | docuSign.com.au

DocuSign is a registered trademark of DocuSign, Inc. All other trademarks are the property of their respective owners. © 2014 DocuSign, Inc. All rights reserved. DocuSign, the DocuSign logo, and On to keep life and business moving forward are trademarks of DocuSign, Inc. All other trademarks are the property of their respective owners. DocuSign, the DocuSign logo, and On to keep life and business moving forward are trademarks of DocuSign, Inc. All other trademarks are the property of their respective owners. DocuSign, the DocuSign logo, and On to keep life and business moving forward are trademarks of DocuSign, Inc. All other trademarks are the property of their respective owners.

b. *The state seeks to achieve reduced or simplified sign-on capabilities. Describe how the solution supports reduced or simplified sign-on.*

DocuSign is capable of integrating with your state's active directories via single sign on (SSO).

c. *It is possible that there will exist multiple identity stores or vaults. Explain the solution's capacity to handle federated identity.*

Depending on the context, there are multiple answers to this question.

1. DocuSign is SAML2 compliant and will support single sign on allowing a federated identity to be used for access to the DocuSign Web Application and for signing a DocuSign transaction. We can also support identity management solutions such as OKTA.
2. Embedded signing allows the ability for the sender to handle the authentication of the signer and federate access to the DocuSign signing session.

7. Architecture

The state prefers a cloud-based, software as a service (SaaS) solution; therefore, please address the following:

a. *What is the solution's SaaS architecture model?*

Please refer to the DocuSign Security Trust and Assurance Packet submitted separately for details on DocuSign's architecture model.

b. *Provide examples of scalability for very large organizations and numbers of concurrent and daily transactions.*

DocuSign has a robust, scalable solution for our electronic signature platform. On average, more than 1.1 million transactions are DocuSigned per day, which is less than 20% of our deployed capacity. DocuSign's product offering can scale both horizontally and vertically. Each tier can scale independently of the other tiers allowing DocuSign to address bottleneck related issues at the source of the problem. Additionally, DocuSign has architected our product to scale to multiple site instances to allow us to scale geographically and to split load to multiple sites.

A great example of capacity would be a large US cell phone provider, who use DocuSign across their retail estate in the US. During the launch of the iPhone 6, we were processing over 100,000 transactions per hour across multiple channels. They were the only US carrier not to suffer system outages during this time and gained market share from their competitors. This provider now forecasts savings of over \$200 million over the next three years by using the DocuSign platform.

c. *Describe how the application performs under load, both in terms of number the number of users and the transaction volume.*

Load spikes are handled by scaling the platform both vertically and horizontally according to usage trends and contractual commitments with an 18-month moving window. Meanwhile, the secured multi-tenant structure ensures that the platform runs at much less than 50% of total capacity and that no one customer's spike in usage impinges on other customers. As data is replicated in near-real-time over dedicated fiber links to each regional-datacenter, user sessions are served using the network-nearest datacenter to improve the user experience. This distributed nature also ensures data resiliency for disaster recovery purposes with an RPO of 5 minutes and an RTO of 15 minutes.

d. *Does the application dynamically scale based on runtime usage and demand?*

Yes, load spikes are handled by scaling the platform both vertically and horizontally according to usage trends and contractual commitments with an 18-month moving window. Meanwhile, the secured multi-tenant structure ensures that the platform runs at much less than 50% of total capacity and that no one customer's spike in usage impinges on other customers.

e. *Provide details to further demonstrate that the proposed architecture and supported platform will scale to meet State current peak and future application processing and user demand.*

DocuSign has a robust, scalable solution for our electronic signature platform. On average, more than 1.1 million transactions are DocuSigned per day, which is less than 20% of our deployed capacity. DocuSign's product offering can scale both horizontally and vertically. Each tier can scale independently of the other tiers allowing DocuSign to address bottleneck related issues at the source of the problem. Additionally, DocuSign has architected our product to scale to multiple site instances to allow us to scale geographically and to split load to multiple sites.

Please refer to the Trust and Assurances Packet submitted separately for additional details on DocuSign's system architecture.

f. *Describe the proposed solution's applications architecture, including offline capabilities, multi-language support, and interface standard supported.*

Please refer to the Trust and Assurances Packet submitted separately for additional details on DocuSign's system architecture.

Offline Capabilities

DocuSign supports the following offline capabilities through a mobile device. DocuSign *is the only vendor to enable the following from a mobile device when the mobile device does not have internet access:*

- In-person Signing
- Create Envelope
- Add Document
- Add In-person Signer
- Add Remote Signer
- Local Document Storage
- Enable Offline Mode

Sign DocuSign in 43 localized languages

DocuSign offers users the ability to sign documents in 43 localized languages. Languages are detected through browser settings, and document senders can also configure language settings accordingly. These include: English (U.S.), Arabic, Bahasa Indonesia, Bahasa Melayu, British English, Bulgarian, Chinese Simplified, Chinese Traditional, Croatian, Czech, Danish, Dutch, Estonian, Farsi, Finnish, French, French (Canada), German, Greek, Hebrew, Hindi, Hungarian, Italian, Japanese, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese (Brazil), Portuguese (Portugal), Romanian, Russian, Serbian-Latin, Slovakian, Slovenian, Spanish (Latin America), Spanish (Spain - Modern Sort), Swedish, Thai, Turkish, Ukrainian and Vietnamese.

Send in DocuSign with 13 languages

DocuSign makes it easy for global users to send documents for signature in their native language. DocuSign offers 13 sending languages, including U.S. English. Languages are detected through browser settings, and can also be configured within Administration tools. Languages include: English (U.S.), Chinese Simplified, Chinese Traditional, Dutch, French, German, Italian, Japanese, Korean, Portuguese (Brazil), Portuguese (Portugal), Russian, and Spanish

Interface

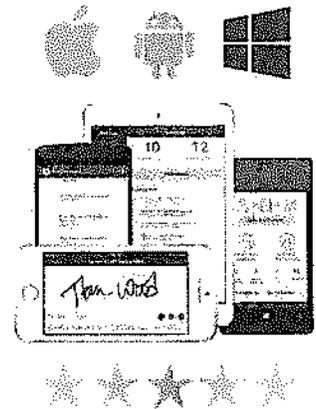
DocuSign has been engineered to be a very intuitive product to use for signers. DocuSign has hundreds of millions of users, with a large number using DocuSign for the first time every day and an enormous effort has been made to make the signing experience very easy and intuitive for all signers. DocuSign is specifically engineered and tested to work for signers on regardless of device type. It recognizes the device and may alter the HTML-5 rendered interface accordingly for the device being used to sign the document. We currently support signing on all HTML-5 capable browsers and mobile devices. In addition, we provide a native SENDING application for iOS and Android.

g. Describe the solution as related to smart devices and operations on smart devices including but not limited to smart pads, smart phones on various platforms. Include limitations in functionality, security, need for installation of facilitating software (apps) and possible additional costs.

DocuSign is specifically engineered and tested to work for signers on regardless of device type. It recognizes the device and may alter the HTML-5 rendered interface accordingly for the device being used to sign the document. We currently support signing on all HTML-5 capable browsers and mobile devices. Additionally, DocuSign is the only platform that offers native mobiles apps for all major platforms: iOS (iPad/iPhone) and Android. DocuSign is available through the Blackberry mobile browser but is not available through a native Blackberry mobile application.

Access your DocuSign account directly from your computer or your mobile device. Sign documents, send documents out for signature, gather signatures in-person, monitor document status, access completed documents and much more. Whether you are in the office, at home, or on-the-go – DocuSign works every time from every device. Additionally, you can access from mobile browsers as well as from our native Apps.

- Support BYOD with native apps for all major platforms
- Quickly sign and send documents from the road—even without an internet connection
- Automate signature workflows into your company's mobile app with the DocuSign Mobile Client Library
- Meet the highest mobile device management standards
- Receive instant transaction updates
- Apps available for iOS and Android.



With DocuSign's mobile apps:

- Sign and send documents from anywhere
- Easily manage your documents, including void and remind
- Real-time status updates provide instant visibility

Offline Mobile capabilities –DocuSign is the only vendor to enable the following from a mobile device when the mobile device does not have internet access:

- In-person Signing
- Create Envelope
- Add Document
- Add In-person Signer
- Add Remote Signer
- Local Document Storage
- Enable Offline Mode

8. Interoperability and Integration

The proposed solution may be required to interface with a variety of other systems. In consideration of this need, respond to the following:

a. *Please describe in detail what type of integration the solution supports; i.e., the integration architecture.*

DocuSign offers a comprehensive set of Web Services APIs in REST and SOAP format. We also provide a variety of Software Development Kits (SDKs) to assist in the use of APIs. More detailed information can be found here:

<https://www.docusign.com/developer-center>

With a 1,000 API calls per hour capacity, DocuSign's API can be used to handle the automation needs of your organization. Automated sending actions can be achieved via 3rd part applications from the individual Sender as well as centralizing the activity via a Send on Behalf Of scenario. APIs can call upon predefined forms (called templates) that may contain form fields that can be prefilled from data in other systems. Based on the need, APIs can be used to check statuses of the document(s) while in-flight and upon completion.

Many organizations also utilize the API capabilities to pull down the documents, transaction details, and/or field data to parse accordingly within internal systems/storage environments. The documents that are pulled out of DocuSign are presented as tamper-evident sealed PDFs with searchable data.

REST API

The following Swagger-generated open source SDKs and tools wrap the eSignature REST API and provide access to all publicly available endpoints and data models at the service layer:

- C# SDK
- Java SDK
- Objective-C SDK
- Node SDK
- PHP SDK
- Python SDK
- Ruby SDK
- Postman eSign API Collection

The iOS-offline-templates-SDK is a dynamic framework that provides native sending/signing UI components and is the first and only DocuSign SDK that supports offline signing:

- [NEW] iOS Offline Templates SDK

SOAP API

The following SDKs can be used to integrate the DocuSign eSignature SOAP API into your apps and websites:

- Java/NET/PHP/Ruby/Apex SDK

Our new Python and Ruby SDKs are part of our Swagger tools family – meaning just like our C#, Java, Node.js, PHP, and Obj-C SDKs they provide access to all public REST API endpoints and data models. They are also open source and licensed under the MIT license.

If you're developing a mobile iOS app and are utilizing template driven document workflows you'll want to check out our new iOS Offline Templates SDK. This is the first and only SDK that provides offline signing API access – allowing your users to

sign while not connected to the internet. (Note: Offline signing is not available on all plans). Additionally, this SDK provides sending and signing UI components that can be integrated into your app in as little as 30 lines of code.

The DocuSign advantage is clear.

DocuSign APIs	Other eSignature Provider's APIs
✓ #1 rated and most powerful REST and SOAP APIs (per ProgrammableWeb)	- Lower-rated APIs (Per Programmable Web), "no other products come close"
✓ REST & SOAP APIs, 3,500+ certified customer integrations, robust sample code, documentation, and developer support	- Minimal sample code and documentation available
✓ 10 SDKs (including iOS Mobile SDK – including offline)	- No robust SDKs available, no iOS mobile SDK
✓ 90%+ developer mindshare on Stack Overflow and presence on Git Hub	- < 5% developer mindshare on Stack Overflow,
✓ Almost 60% of transactions completed using the DocuSign API	- < 33% of transactions completed using the API

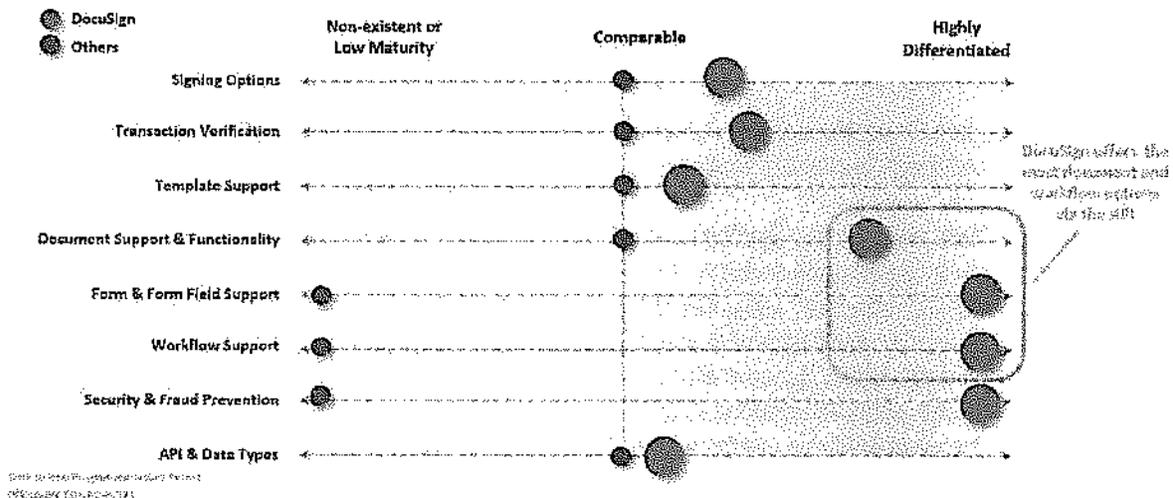
Customers can easily create custom applications using a multitude of developer resources at their disposal to do so. DocuSign can also create these applications on customer's behalf. DocuSign is the only vendor to support integrations with six different SDKs, including the only vendor to provide customers with an iOS mobile SDK for custom app integration on Apple devices.

DocuSign was rated the #1 eSignature API by ProgrammableWeb, the leading API industry analyst firm.

ProgrammableWeb is quoted as saying in the report that **"It's hard to look closely at these products and not conclude that DocuSign is in a class by itself. The DocuSign API is far more comprehensive than the rest. The documentation, sample code, tools, and community are superior to that of all the other products. And no other product came close..."**
"Our evaluation showed that DocuSign has the greatest breadth of features available under the API, the best developer tools and the best code samples and documentation."

ProgrammableWeb Rankings of DocuSign's API

DocuSign's APIs are ranked #1 in every category



DocuSign has over 90% mindshare of all eSignature solutions on Stackoverflow.com and has the largest developer community by many multiples with over 80,000 developers accounts registered. DocuSign has completed and certified more than 3,500 customer integrations, far more than any other vendor.

DocuSign's service is accessible via an open and published API. DocuSign supports both SOAP and REST APIs that allow customers to easily and quickly integrate any of DocuSign's features into systems including workflow. Mobile channels can make use of DocuSign's open APIs. DocuSign's REST API offers a lightweight interface conceived for use with mobile devices and has been used by several customers in the development of powerful, mobile solutions. DocuSign has also delivered the industry's first Mobile SDK for iOS that enables mobile developers to build Digital Transaction Management (DTM) and electronic signing capabilities natively into mobile apps. More information can be found at <https://www.docusign.com/developer-center>.

b. Solution provides Application Programming Interfaces (APIs) for integration with other Customer systems. Include any details on Application Programming Interfaces (APIs) provided. Some of the potential integrations are:

- SAP (SAP SSO cookies for example)
- Web services (MQ Series, other APIs)
- Enterprise Service Bus (e.g. Web Sphere Service Broker)
- LDAP (for authentication)
- NCID (for identity management)
- Document management systems (list)
- Office software packages (Office 365)
- Business systems such as human resources, accounting, finance, CRM, ERP, LMS, etc.
- SharePoint Online and On Premises
- Dynamics 365, Salesforce.com

Yes, DocuSign supports integrations with other customer systems. DocuSign is the only provider with strategic partnerships with Microsoft, Salesforce, Google, Apple, SAP, and IBM, among others. DocuSign has the largest partner ecosystem in the industry, multiples larger than any other vendor. DocuSign's partner ecosystem is another one of DocuSign's key

differentiators. With more than 350 partner integrations in a variety of industries and use cases – and pre-built connectors with solutions from vendors such as SAP, Microsoft Office 365, NetSuite, Salesforce, SharePoint, and Dynamics 365 available in our Solution Showcase – you can deploy quickly and save costs. If a connector doesn't exist, customers can leverage the DocuSign Developer Center which already has over 80,000 developers using our open APIs. Customers can also leverage The DocuSign Partner Directory for a certified DocuSign consulting partner to deploy DocuSign or build custom solutions.

Microsoft

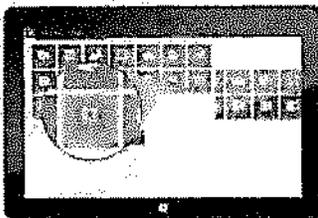
Through a long-term strategic partnership with Microsoft, DocuSign has made its industry-leading eSignature apps and Digital Transaction Management functionalities widely available to businesses and consumers within Microsoft applications.

Robust apps for Outlook, Word, SharePoint, Dynamics 365 CRM, and Windows are making it easier for organizations of every size, industry, and geography to quickly and securely transact business anytime, anywhere, on any device.

Microsoft is a long-time DocuSign customer, using DocuSign in more than 316 use cases around the world. These use cases were made possible by DocuSign's robust technical capabilities, legal compliance, and unmatched security platform. Microsoft has worked diligently with our U.S. based Account Management and Customer Success Architect teams. DocuSign and Microsoft continue to identify use cases to continue to streamline their workforce of over 115,000 employees worldwide. As recognition for its overall user experience, performance and integration into Microsoft Office and SharePoint, DocuSign's eSignature and Digital Transaction Management (DTM) platform were awarded first place winner in the Best Mobile App award as part of the Office App Awards at Microsoft Ignite 2016. DocuSign was recognized as the 2014 Microsoft Office and SharePoint App Developer Partner of the Year Award.

How You Can Use DocuSign with Microsoft

Out of the Box Integrations



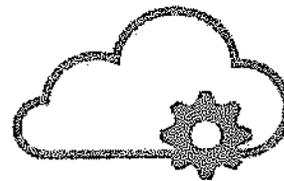
DocuSign for Word
DocuSign for SharePoint
DocuSign for Outlooks
DocuSign for Dynamics CRM

Mobile & Desktop App



DocuSign for Windows 10
DocuSign for Windows 8.1

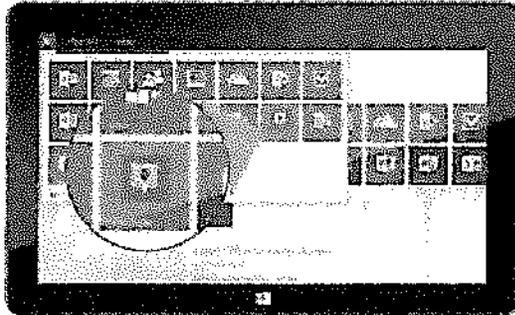
API



Customize using leading APIs

DocuSign for Microsoft

Use DocuSign right from the applications you're using everyday



- Easily install from Office Store, Microsoft Store or PinPoint
- Single Sign in with O365 credentials, powered by Azure Active Directory.
- Save completed documents to OneDrive for Business
- ✓ Improve productivity for entire organization by reducing steps to DocuSign
- ✓ Ensure all contracts and agreements across your org and secure, tracked and saved centrally
- ✓ Control and manage business agreements and contracts
- ✓ Eliminate paper and enable a digital workplace
- ✓ Increase the use of existing investments

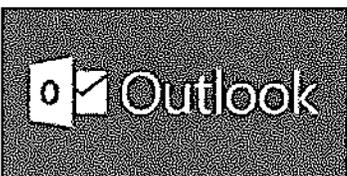
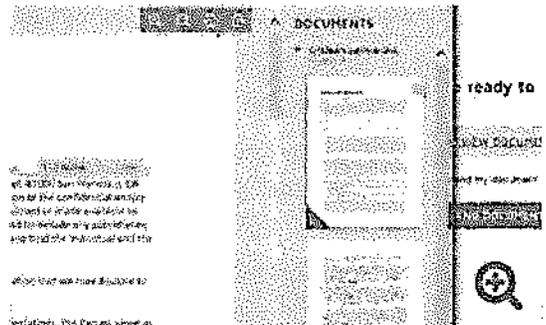


DocuSign for Word

DocuSign for Word enables you to get signatures and sign important documents securely from Word—anytime, anywhere—in minutes.

Key Features

- **Create and edit a document, sign, or send for signature.** Sign or request signatures on any document created or edited in Word 2016. Drag and drop tags where recipients need to sign, or securely sign a document yourself.
- **Streamline business processes.** Easily edit a document using Microsoft Word and use DocuSign to specify the signing process to route the document to the right people in the right order.
- **No new set up required.** Log in with your existing Microsoft account or Office 365 credentials and use DocuSign without ever leaving Word.
- **Access on the go anytime, anywhere.** You and your customers can get your documents DocuSigned from any device without downloading another app.
- **Secure storage built-in.** Once all recipients have signed, automatically save completed documents in a DocuSign documents folder in OneDrive or OneDrive for Business for easy access.



DocuSign for Outlook

DocuSign is the only vendor with a Microsoft Outlook integration or application. Other vendors may claim an integration with Microsoft Outlook in some form through services not related to eSignature, but DocuSign is the only vendor that offers and integration with Microsoft Outlook that lets users send documents for signature directly from Microsoft Outlook. DocuSign is the only vendor that supports the following Microsoft Outlook:

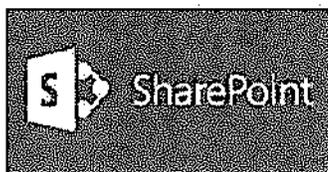
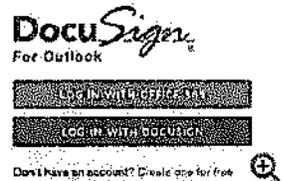
SOLICITATION # ITS-400335

- Support for Outlook Web App, Outlook 2013 desktop (Windows only), and Outlook 2016 desktop; as well as Internet Explorer 11, and latest versions of Firefox, Edge, and Chrome
- Sign, send, manage and specify mixed routing workflows
- Save copies of Document to Microsoft OneDrive for Business
- Send or sign in 13 languages
- Auto-sync with Microsoft Azure Active Directory
- Admin controls and management for MS Exchange admins

DocuSign has out of the box integration with Microsoft Word and Outlook delivered through Office 365. For more information, please see our Solutions Partner page for DocuSign for Microsoft: <https://www.docusign.com/solutions/microsoft> With DocuSign for Outlook, organizations of all sizes can increase productivity, reduce costs and improve customer experience by enabling individuals and organizations to legally and securely sign and return documents directly from their Outlook inbox.

Key Features

- **Manage email attachments more efficiently:** Eliminate the need to print, scan, fax, or send documents overnight by securely signing and returning documents without ever leaving your Outlook inbox. If you need others to sign the document, specify the recipients and tag the document using DocuSign directly from the app.
- **Easy access from your inbox:** Access DocuSign from the Outlook apps toolbar by logging into your existing DocuSign account or create a new one using your existing Office 365 credentials. Your accounts are automatically synched using single sign-on capabilities powered by Azure Active Directory.
- **Easily send documents out for signing from Outlook:** Start the signing process from the new mail/reply window, just like you're writing a new email. Simply upload your documents and DocuSign for Outlook prepopulates signers from your email message.
- **Built-in document storage:** Connect your DocuSign account with your Office 365 credentials and automatically save copies of completed documents to OneDrive for Business for easy, centralized access.
- **Administrative controls and management:** Administrators can easily manage DocuSign for Outlook for any organization. Grant access, easily add and remove users, and manage and configure permissions and controls. Ensure compliance and maintain a centralized, secure location for all DocuSigned documents throughout your organization.

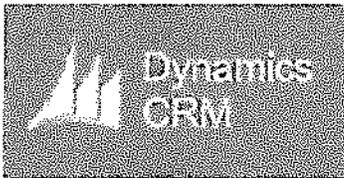


DocuSign for SharePoint

Collaborate better with fast, secure electronic signatures. DocuSign for SharePoint Online allows users to easily sign or get signatures on any document stored in a SharePoint document library, manage documents centrally and collaborate with customers, employees, and partners more efficiently.

Key Features

- **Easily send and sign documents.** Sign and send out documents for electronic signature using DocuSign for SharePoint Online. Documents in the SharePoint Online library can be easily sent, signed, and managed by selecting the DocuSign tab in the ribbon bar.
- **Automate existing business processes.** You can easily automate existing business processes and workflows. Easily select documents in the SharePoint library for signing or sending, and use DocuSign to specify signing workflow to route your document to the right people in the order you choose.
- **Track status of documents.** Use your existing company credentials to sign into DocuSign without leaving SharePoint or create a new DocuSign account using your Office 365 credentials. Accounts are automatically linked using single sign-on capabilities powered by Azure Active Directory.
- **Administrative controls and management.** Easily manage administrative controls with DocuSign for SharePoint Online. Grant access, manage users, ensure compliance and maintain a centralized and secure location for all DocuSigned documents across your organization.



DocuSign for Dynamics 365 CRM

DocuSign for Dynamics 365 CRM helps Microsoft Dynamics 365 CRM customers send contracts for signature directly from the application. Your customers can sign documents from any browser — including mobile devices — within minutes, and update Dynamics 365 CRM data at the same time. Delight your customers and close deals faster.

Key Features

- **Get signatures or sign documents with ease.** Signing or getting signatures on a document is simple using DocuSign for Dynamics 365 CRM. The "Sign" and "Get Signatures" actions are preconfigured, allowing you to easily send or sign a document stored in DocuSign for Dynamics 365 CRM, pre-populated with appropriate recipient information.
- **Gain more control and visibility into your sales process.** DocuSign for Dynamics 365 CRM provides an audit trail of edits and notifies every signer when a document is changed – giving your users visibility into the entire process.
- **Designed for sales with easy integration.** Created with sales departments in mind, DocuSign for Dynamics 365 CRM helps you close business faster. Route contracts to the people you choose, allowing decision makers to review and approve contracts within minutes. Signed agreements are legally binding and backed by a court-admissible audit trail.
- **Easy to configure and customize.** DocuSign for Dynamics 365 CRM is a platform designed and built for flexibility. It can be configured and customized to integrate with most business processes. DocuSign ships a complete set of APIs along with documentation and world-class SDK.

DocuSign Transaction Associati

+ ADD NEW DOCUSIGN TR... + ADD EXISTING DOCUSIGN

Created By	Created On	Envelope Stat...
Lahiri Arunacha...	1/5/2015 2:16 PM	sent
Lahiri Arunacha...	1/5/2015 2:48 PM	created
Lahiri Arunacha...	1/5/2015 3:01 PM	delivered

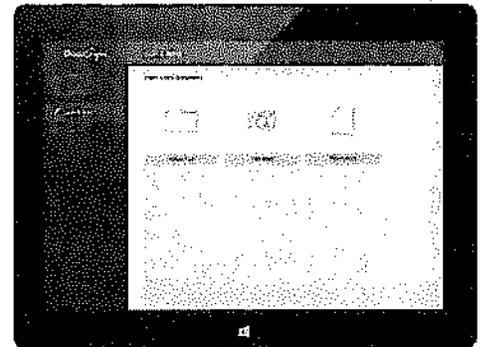


DocuSign for Windows

Send and sign documents on your Windows device. DocuSign for Windows makes it easy to sign a document and get signatures on the go. Finish tasks faster and go completely paperless – no more printing, faxing, scanning or overnighting documents for signature.

Key Features

- **Sign and send documents in multiple formats.** You can sign and send nearly all document formats – including Microsoft Office documents, PDFs, image files, and documents stored on cloud storage apps like OneDrive for Business, Box, and Google Drive. Simply drag and drop or upload any document that requires a signature – directly from your Windows 10 device.
- **Keep track of all your documents.** View and track all your documents to see who has signed, and follow up on documents waiting for a signature, giving you complete visibility and control. With the Windows live tile, you can see your critical document status directly from your desktop or home screen.
- **Secure and legally binding.** Choose the solution trusted by banks and law firms. DocuSign e-signatures are safe, secure and legally binding. All documents are encrypted and include a tamper-proof seal and complete transaction history.
- **New features for Windows 10.** Enjoy several new features including People Hub integration and enhanced digital inking capabilities, making sending and signing more personal than ever. DocuSign for Windows 10 is fully responsive, meaning that you can work in full-screen mode, or in a smaller window on your desktop.



Salesforce

Our longest running strategic partnership is with Salesforce which is a strategic investor in DocuSign, and deployed DocuSign enterprise-wide internally, and offers tight integration with their Professional, Enterprise, Unlimited, Force.com, and Developer editions of Salesforce.com. DocuSign was a launch-partner for the Salesforce1 mobile app; Salesforce users can close business on the go. In fact, DocuSign is the most popular electronic signature app on the Salesforce AppExchange. As part of our integration with the Salesforce platform, we integrate with most major force.com ISVs.

SOLICITATION # ITS-400335

Using the global standard for Digital Transaction Management, DocuSign® for Salesforce® is the easiest, fastest, most secure way to send, sign, track and store documents in the cloud. Fully integrated with Salesforce, DocuSign helps users close more deals, faster. Your customers can sign contracts within minutes from anywhere, anytime and on any device.

The eSignature Choice for Salesforce

DocuSign is the #1 electronic signature solution and is used exclusively by Salesforce's over 3,000 Salesforce with 45+ internal use cases around the world. The results speak for themselves, over 90% of all Salesforce's contracts sent through DocuSign are returned within one day, over 71% within one hour. LinkedIn, Expedia, CenturyLink, Xerox and more than 40

million people and enterprises trust DocuSign to accelerate the speed of their business. Sending a contract for electronic signature from Salesforce is simple: Just click "Send with DocuSign" from any object. You can even generate and send contracts synced with data from Salesforce. When you automate time-consuming manual workflows, you eliminate rekeying of data and increase your productivity. DocuSign handles many different scenarios, including:

Multiple signers

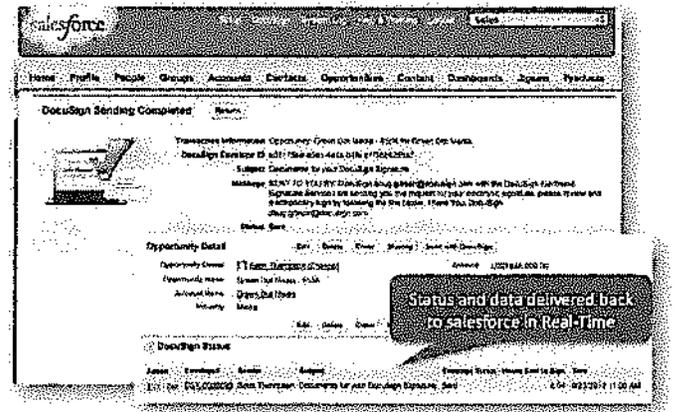
Confirmation of a signer's authority to sign

Specified signer routing order

Designation of specific fields as negotiable

Delegation of signing responsibility to others

Signing in person and on mobile devices



Further evidence of DocuSign's strong partnership and strength of integration with Salesforce is in our numbers.

- DocuSign is the most-downloaded App on the AppExchange (all-time)
- 5,200 companies currently use the DocuSign/Salesforce connector
- DocuSign is the 4th top-grossing ISV partner (and the #1 non-consulting firm)
- DocuSign is the only e-Signature provider featured in the Salesforce Simple Demo Org
- DocuSign is used exclusively in Salesforce.

DocuSign for Salesforce Customers



58

DocuSign® allows you to send, sign, and approve documents from wherever life takes you.

DocuSign enables organizations of any size to securely send, sign, track, and store business-critical documents directly within Salesforce. DocuSign for Salesforce helps increase employee productivity by enabling faster transactions and keeping business processes digital from end to end. The solutions are deployed through the cloud and are available to all your users anywhere, anytime, and on any device. DocuSign is secure, legally enforceable around the globe, and can reduce business risk by ensuring compliance with various policies and regulations. <https://www.docusign.com/solutions/salesforce>

Key Features

- Intelligent template recognition helps you get your most-used documents out the door, faster.
- The most downloaded app on the Salesforce AppExchange & a Salesforce Platinum Partner
- #1 e-Signature solution & exclusively used by Salesforce.com
- Lightning ready (for more information, see <https://www.docusign.com/sites/default/files/DocuSign%20SalesForce%20Lightning%20Datasheet.pdf>)
- Works across Salesforce Cloud Solutions, including Sales Cloud, Service Cloud, Salesforce CPQ, and Communities
- Merge data from any object
- Streamline routing with automated workflows
- Two-way data flow eliminates manual data entry
- Sign in-person, or on any device
- Increased pipeline visibility with real-time updates via Chatter

SAP/Ariba

SAP helps organizations fight the damaging effects of complexity, generate new opportunities for relationships and growth, and stay ahead of the competition.

SAP has a long-term relationship with DocuSign as a customer, partner, and investor.



DocuSign and SAP have partnered together to enable businesses of every size, industry, and geography to go 100 percent digital. Integrations with Ariba Contract Management and SuccessFactors Recruiting Management allow customers to leverage SAP technology with DocuSign's Digital Transaction Management platform to "Run Simple".

Ariba Contract Management



Go ink- and paper-free with electronic signatures, and watch your savings, revenue, and productivity growth.

Delivered via the Ariba Commerce Cloud, Ariba Contract Management is the market-leading SaaS solution for all stakeholders addressing all enterprise-wide agreement (procurement contracts, sales contracts, intellectual property licenses, employee agreements, etc.).

On a single, user-friendly platform, users can standardize and accelerate the process, from initial request to contract authoring and creation, to negotiation and approvals and storage. Ariba also offers the advantage to negotiate with buyers and sellers from the world's largest online trading partner community while driving efficiency and compliance by integrating contract management processes with spend management and customer relationship management (CRM) solutions.

For contract execution, Ariba has partnered with DocuSign for the leading electronic contract execution capabilities available today permitting users to gain the efficiency and cost benefits of eSignatures seamlessly making the contracting process truly paperless.

Close deals faster and more efficiently with electronic signatures. An electronic signature is a fast and secure way to sign a contract. It involves attaching an encoded signature to an electronic document, verifying the identity of the signer and signifying an approval to terms. By eliminating all the paper and administrative hassles, DocuSign customers have reduced to mere minutes the time it takes to execute a contract, and enjoy...

- Average of 80% reduction in turnaround time
- \$20 average savings per document
- Accelerate document signing from 1-2 weeks to <1 day

For more information:

<https://www.docusign.com/sites/default/files/DocuSign-For-Ariba-Overview.pdf>

<https://www.ariba.com/>

SuccessFactors Recruiting Management



SuccessFactors Recruiting Management Online Offer with eSignature provides clients with the ability to collect electronic signatures from candidates to help improve the overall candidate engagement experience and eliminate the need for manual, paper-based processing.

Clients can allow permissioned Recruiting Users to create and send Online Offers requesting an electronic signature from candidates within the Career Portal, using DocuSign.

Key Features

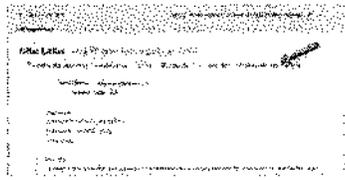
- Send offer letters from within SuccessFactors Recruiting Application to any candidate with an email address
- View the completed and in process offer letter within the SuccessFactors Recruiting Application

By eliminating all the paper and administrative hassle, DocuSign customers have streamlined their HR operations with an electronic signature, saving time, reducing errors, and increasing compliance and user experience. By eliminating all the paper and administrative hassles, DocuSign customers have enjoyed...

- \$14.9 saved per new hire document, offer letter, and onboarding form
- Average turnaround time reduced from one week to less than a day
- Offer letters and paperwork returned with zero incomplete fields

Key end-user features

Online Offer with eSignature



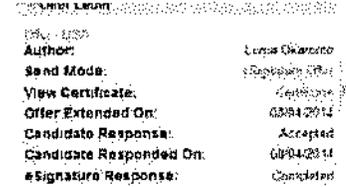
- Eliminate the need to print and overnight offer letters by sending and having them returned electronically through DocuSign
- User able to use DocuSign directly within the SuccessFactors system

DocuSign Tagging Console



- Candidate email and message to be sent is prepopulated with the offer letter template
- Drag and drop tags onto the document for the candidate to complete
- Additional documents and signers can be added within DocuSign

Offer Letter Portlet



- Track the status of any job offers that was sent for eSignature directly from SuccessFactors
- Ability to view history of the signing process for both completed and standing job offers

For additional information, please see

https://na87.salesforce.com/sfc/p/#300000000bS4/a/40000000PbE5/CBHBuC_BriAZP39IldIEttKQT_Kg3E73ftqcK14Uk_s=
<https://na87.salesforce.com/sfc/p/#300000000bS4/a/40000000PguB/RdwENX6QILzC1MhCWstozfBv5ALpNZX9hI4L93xcp0>

SAP Hybris

SAP Hybris

With SAP Signature Management by DocuSign, you can digitize manual, paper-based recruiting and onboarding processes and manage end-to-end in the cloud. It is one of the only electronic signature management solutions that can securely automate workflows, collect information and obtain legally binding signatures from anywhere in the world. Use it to

streamline processes, reduce costs, improve compliance, present a positive company image, and delight candidates.

For more information:

<https://www.sapappcenter.com/apps/5473#!resources>

c. *Are APIs secure and encrypted? What Encryption Method,*

Yes, all access to our web services API are over a TLS encrypted connection. To use an API, a password, ID and integrator key must be provided or alternatively, an OAuth user token.

d. *How do you extract form or record data? Do you use industry standards such as XML?*

All form and record data is intelligent metadata that can be extracted from the system. The typical extraction formats for the data are in CSV or XML.

e. *How is data inserted into a form? Can data be inserted dynamically (based on user inserted data)?*

Data can be inserted into a form manually or via an automated interaction from another system. If the manual process is used, "Signers" enter the data via the browser and if duplication of data needs to happen in other fields, that can be set up to automatically happen. There is also the ability to initiate the process from another system that can automatically fill-in information as needed.

DocuSign provides for 'Conditional Logic' on the data and fields that are entered in the transaction. Based on the answer(s), fields (tags) can dynamically appear/disappear as well as be set to handle specific data (validated format). This can be designated based on selection of certain data, radio buttons, checkboxes, or any/specific data within text fields.

f. *Can forms be processed via API in both real time and/or batch mode?*

Yes, using APIs can provide the ability to have transaction processes handled in real-time or in batch based on the need for the state/agency.

g. *How does the API deal with multiple accounts (for enterprise-wide forms)?*

There are no issues with using multiple accounts with the DocuSign API. API calls are generally made by a system account and ID and have the option of being made on behalf of a member in the account.

h. *Can the API retrieve software version numbers?*

Yes, DocuSign's API can retrieve software version numbers.

i. *How are fields identified in the API?*

To DocuSign, "fields" describe data fields on a form. With that definition, there are three primary operations clients perform with DocuSign fields via the API:

1. Populate fields with data
2. Read field data from the completed transaction
3. Create fields in a new transaction

Fields have several attributes in DocuSign, the most essential being their name and value. In the first two operations above, the process of identifying fields for the purpose of populating or reading data from them is via name/value pairs. The third operation pertains to creating fields within a DocuSign transaction. Fields can be created via a design-time, drag-and-drop authoring tool in a DocuSign Template; by transforming fields from a fillable PDF into their DocuSign equivalents; or by expressing them verbosely via the API. In any of those cases, other field properties are established regarding their field type, position, optionality, conditionality, ownership, font-style, data type, and other attributes that determine their behaviors when presented. Within the DocuSign API, fields are defined through *Tab* objects.

j. *How is the workflow engine capable of easily supporting a variety of e-forms?*

DocuSign provides the capability to handle multiple templates that will allow agencies to handle a variety of forms. With the extensive field tags, you are able to handle the acquisition of data, signatures, initials, etc. The solution provides flexibility of the workflow. For more consistently used documentation, templates can be created and managed locally by users who have the permissions to do so. This will allow for the setting of specific user(s) and or groups for signing at defined times within the workflow.

k. *The state prefers REST web service interfaces. XML schemas should be derived from industry standard vocabularies where possible such as the National Information Exchange Model (NIEM). Describe how the solution will support these and other interoperability standards.*

DocuSign offers a comprehensive set of Web Services APIs in REST and SOAP format. We also provide a variety of Software Development Kits (SDKs) to assist in the use of APIs. More detailed information can be found here: <https://www.docusign.com/developer-center>

9. Applications Management and Control

Describe the process of raising and managing exceptions within the application. Please include the following:

a. *Address whether multifactor authentication (MFA) access is available for all accounts including signatories, admins, and form builders? Is it included in the price? If not provide pricing in the cost section.*

For users who are not enrolled in NCID (external signers) multifactor authentication is available.

For users that are enrolled in NCID, Single Sign On (SSO) redirects these users to NCID for authentication and NCID can set up MFA for these users.

Access codes are free, paid options are listed in the Cost Section.

b. *Describe the level of customer control on the timing of applying patches, upgrades, and changes to the SaaS application and the notification process to be used.*

While DocuSign is a service and updates are applied to platform, major changes that affect the overall experience or function of DocuSign are not "forced" in this way and are opt in with a timeline to being implemented across the board. A good example of this would be our redesign of our signing experience. While it was launched and available in the platform, DocuSign provided an 18 month runway for Customers to test and adapt to the new functionality to ensure integrations and experiences would not be affected. This is a common approach to major changes with DocuSign.

Patches are obtained from vendors and deployed on a monthly basis across all production environments and network vulnerability scans are conducted afterward. Emergency patches are immediately applied as needed and follow Change Management procedures.

c. *Explain the process for handling software defects.*

DocuSign uses an issue tracking solution to capture and prioritize solution defects as well as product enhancements. Overall, the defect rates for the solution are incredibly low. Additional information about the system performance for DocuSign can be found at: <https://trust.docusign.com/>.

d. *Describe the major and minor release policy for the solution.*

DocuSign has a well-established product release cadence. These include four (4) seasonal releases annually, along with monthly service packs. As part of each seasonal release, DocuSign provides in-depth information about new capabilities to help customers rapidly realize the benefits within their organization. As an example, please refer to the DocuSign Winter '17 Release (<https://www.docusign.com/support/releases>) as a representative example of the type of information we share with customers upon each release. DocuSign is confident that our current capabilities will support the needs of your organization. However, we understand business evolves quickly, especially in the face of innovation. DocuSign recognizes the significance that innovation can play in changing your business. As such, DocuSign has taken the holistic approach described above so that we can establish a mutually beneficial long-term relationship with you.

e. Describe user configuration capabilities.

Please see the DocuSign Administrator Guide at <https://support.docusign.com/en/guides/ndse-admin-guide>. Since this is a broad question and DocuSign has many capabilities in this area, we included the link for the State to explore. This document is over 300+ pages and is too long to include in our response. Additional information on any specific capability can be provided if requested.

f. Describe user self-provisioning capabilities.

The DocuSign platform is designed with an emphasis on self-sufficiency for our customers. As such, some Users within the customer Account will have Administrative privileges to create Users. This process can be performed via DocuSign's Admin experience as either one-off or bulk operations; via the API through custom application development; or via Single Sign-On auto-provisioning rules.

g. Describe the level and skill set needed by the State to administer and configure the proposed solution.

Administering DocuSign requires the execution of basic operations procedures and does not require any specific programming or technology skills. Most administrative functionality e.g., provisioning new users, maintaining groups, building templates can be done interactively using the DocuSign Web Application.

Additionally, DocuSign offers free training courses, including a full course list for Administrators to help speed the implementation process and improve the administration. These courses include self-paced and live, instructor-led workshops. Please see <https://support.docusign.com/docusignuniversity> for more information. Please see XXX which provides a detailed list of suggested training courses for Administrators. This will help State Administrators use DocuSign to its full advantage without minimal ease.

h. How do you address Delegation of authority?

Delegated Administration empowers IT, business analysts & others to administer specific functionality within your account while maintaining control. Permissions include the ability to manage:

- Users, Groups, Admins, and/or Document sharing
- More permissions coming soon

Directly access the New Admin Experience via URL and manage volumes of data.

At a high level, Delegated Admin provides customers with the ability to create account structure and permission sets, so they can manage users, groups, and admins document sharing, and therefore increased flexibility and visibility. For example, a customer can configure an Admin that only manager's users without access to the documents, or another that can share documents but have no user editing right. In addition, they can access Delegated Admin through the New Admin Experience URL (internally known as RADmin) in an easy-to-navigate UI.

Key Benefits for Delegated Administration

- ✓ Provides maximum flexibility within a scalable, secure, and auditable structure using permission sets
- ✓ Access data through simplified and intuitive UI
- ✓ Audit change history and gain enhanced visibility

Use cases for Delegated Admin

- **Administration-only (Super Admin)** - A role that has all admin rights but no access or limited access to other DocuSign application features
- **IT User Manager** - A role for IT helpdesk or other delegated administrator who can add, update, or close users but nothing else
- **User Manager no sharing** - A role that allows an admin to create, edit, close users, and groups but no access to sharing capabilities

i. Describe how privileged management accounts are secured, provide encrypted authentication and access to authorized users.

Accounts in DocuSign are secured using a user ID and email address. User accounts could be managed with SSO. If SSO is employed, it's possible to mandate a two-2 factor authentication to the account for all account users.

j. Specifically, does the Delegation of Authority capability that allows signatories to delegate signing authority for documents for a specified period of time, or indefinitely.

No. DocuSign does not support a delegation of authority feature at this time. It is possible for a signer to change the ownership of the signing authority to someone else.

10. Application Specifications

Please describe how the solution will include the following application specifications:

a. Describe integration with Microsoft Office 365 Office Productivity & Email.

Through a long-term strategic partnership with Microsoft, DocuSign has made its industry-leading eSignature apps and Digital Transaction Management functionalities widely available to businesses and consumers within Microsoft applications.

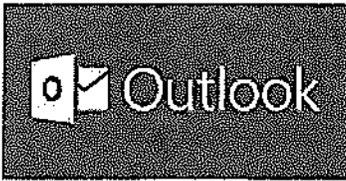
Robust apps for Outlook, Word, SharePoint, Dynamics 365 CRM, and Windows are making it easier for organizations of every size, industry, and geography to quickly and securely transact business anytime, anywhere, on any device.

Microsoft is a long-time DocuSign customer, using DocuSign in more than 316 use cases around the world. These use cases were made possible by DocuSign's robust technical capabilities, legal compliance, and unmatched security platform. Microsoft has worked diligently with our U.S. based Account Management and Customer Success Architect teams. DocuSign and Microsoft continue to identify use cases to continue to streamline their workforce of over 115,000 employees worldwide.

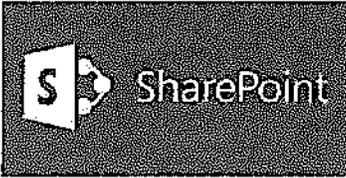
As recognition for its overall user experience, performance and integration into Microsoft Office and SharePoint, DocuSign's eSignature and Digital Transaction Management (DTM) platform were awarded first place winner in the Best Mobile App award as part of the Office App Awards at Microsoft Ignite 2016. DocuSign was recognized as the 2014 Microsoft Office and SharePoint App Developer Partner of the Year Award.



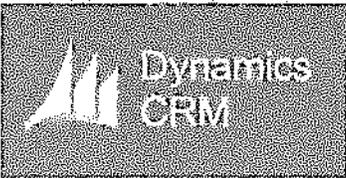
DocuSign for Word - DocuSign for Word is simple to use and enables individuals or organizations of any size to securely send and sign important documents right from Word. Increase productivity and transact faster by keeping business digital.



DocuSign for Outlook - DocuSign for Outlook lets you sign and return any document from Outlook within seconds. DocuSign works seamlessly within Outlook allowing you to collect signatures and other information on documents.



DocuSign for SharePoint - DocuSign for SharePoint enables organizations to legally and securely send, sign, and track important documents stored electronically in SharePoint. Easily access, manage, and control documents from a central location so that you can enhance productivity, transact faster, manage compliance, and keep your business moving.



DocuSign for Dynamics 365 CRM - DocuSign for Dynamics 365 CRM helps Microsoft Dynamics 365 CRM customers send contracts for signature directly from the application. Your customers can sign documents from any browser — including mobile devices — within minutes, and update Dynamics 365 CRM data at the same time. Delight your customers and close deals faster.



DocuSign for Windows - DocuSign for Windows makes it easier than ever to sign a document and get electronic signatures from others. Store and manage all your signed documents with your DocuSign account and OneDrive for Business. Finish tasks faster by going 100% digital.

b. Describe how the solution can initiate the signature process with PDF and Word documents. Please note that the vendor may apply custom branding (official logos, colors, hyperlinks) as necessary to create a consistent user experience. Please see Section III, #6 for more information.

Users are able to upload PDF or Word documents into DocuSign to initiate the signature process.

In addition to PDF and Word documents, DocuSign supports the following file types:

- **DOCUMENT** .as, .asl, .doc, .docm, .docx, .dot, .dotm, .dotx, .htm, .html, .pdf, .pdx, .rtf, .txt, .wpd, .wps, .wpt
- **DRAWING** .dwg, .dxf, .emz, .svg, .svgz, .vdx, .vsd, .vss, .vst
- **IMAGE** .bmp, .cdr, .dcx, .gif, .ico, .jpg, .jpeg, .pct, .pic, .png, .rgb, .sam, .tga, .tif, .tiff, .wpg
- **PRESENTATION** .dps, .dpt, .pot, .potx, .pps, .ppt, .ppim, .pptx
- **SPREADSHEET** .csv, .et, .ett, .xls, .xlsx, .xlt

Google file formats: While Google file formats (Docs, Sheets, and Slides) are not supported in their native format, you can upload these file types if you connect your Google Drive cloud storage to DocuSign. Once you've connected, you can use the cloud storage option to add the Google files to a document. See Give DocuSign Access to Your Cloud Storage for details.

Custom Branding

DocuSign is easily customizable and configurable. One method of customization is by branding. Branding your DocuSign account is an excellent way to add the look and feel of your organization's brand to the sending, signing, and email process making it easier for users to identify envelopes coming from your organization. The DocuSign Account Custom Branding feature lets you set the colors, logo, and text for your account to enhance the sending and signing experience. You can create any number of brand profiles with different settings to reflect each of your corporate brands or different divisions or departments.

When you create or change a branding profile, it applies to everyone using that profile and affects all envelopes sent with that profile.

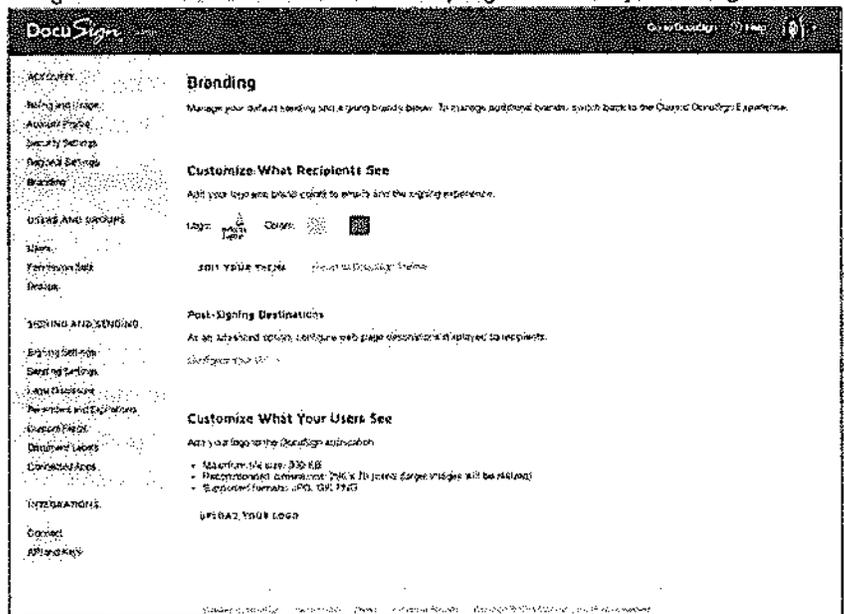
Another approach to customization is using the DocuSign API's. Each function is available programmatically, allowing the customer to create a unique experience, including embedding DocuSign in a custom application (mobile or web-based).

DocuSign is also highly configurable, allowing the customer to create reusable templates, define workflows, save personal reports; for example, without required service from DocuSign. Each DocuSign customer has unique requirements and DocuSign has been designed to be flexible to meet those requirements.

Email Branding

Emails can be customized with the subscriber's logo and color scheme. The email subject and email message can also be customized.

A unique capability of DocuSign is that each recipient in a multi-recipient workflow can receive an individualized email, with different verbiage. In a multi-language scenario, each recipient may also receive a different, localized set of emails. Not only is the UI localized, but the email body itself.



c. Describe how the solution works with Section 508 compliant screen readers and other ADA capabilities. Specifically, in-process and completed documents should be fully read by a screen reader.

DocuSign is the only eSignature vendor to provide support for the PDF/UA standard, which allows for "reading zones", and required for full compliance. This type of document, in conjunction with the DocuSign software, allows the document being signed to be "read" by screen reading technology. Other eSignature vendors lock their documents during signing in a way that screen readers cannot help the disabled know what they are signing. Is it helpful that someone can sign, but not know what they are signing? Only DocuSign is WCAG "AA" certified. Here is a brief video to show the experience:

<https://www.youtube.com/watch?v=-BFcp9H9IHw>

DocuSign is committed to providing our high-quality solution in a manner that is accessible to all individuals, regardless of their abilities. To meet this goal, DocuSign's accessibility support functionality provides all people equal access to and the freedom to interact with DocuSign's signing application when using assistive or adaptive technologies, in accordance with WCAG 2.0 Level AA and U.S. Government Section 508 standards.

SOLICITATION # ITS-400335

- Web screen readers such as JAWS (Job Access with Speech), NVDA (NonVisual Desktop Access), ChromeVox, and VoiceOver with Safari
- Dragon Text to Speech
- Keyboard navigation
- Browser and signing experience zooming tools to provide low-vision signers the ability to magnify documents without any loss of functionality.
- Tool tips and color contrast ratios for visually impaired signers.
- Finish button behavior. When signers select Finish the system performs validation and if any required fields have missing or incorrect data, the system will change the focus to that field and include information about what is wrong.
- Reading zones.

Benefits for the State:

- ✓ Permits all users equal access to sign and send documents, regardless of their abilities
- ✓ Allows blind and vision impaired users the flexibility of signing documents online

As demonstration and verification of our accessibility features, please see our updated VPAT documentation to fully understand the depth of DocuSign's accessibility capabilities.

<https://www.docusign.com/sites/default/files/DocuSign-Voluntary-Product-Accessibility-Template.pdf>

d. Provides a digital signature solution in which the "root" digital certificate is provided by a certificate authority that meets assurance and trust requirements by Adobe. Documents with these certificates become automatically trusted by Adobe as this facilitates the ability to validate the signature. More information about Adobe's Approved Trust List and current members of that list can be found at <http://helpx.adobe.com/acrobat/kb/approved-trust-list2.html>.

All documents exported from DocuSign are digitally signed for the purpose of tamper evidence. The tamper seal is an X.509 PKI standards based "Digital Signature" that is applied to the document at the time it is downloaded from DocuSign. The mechanism would indicate if the document has been changed since being downloaded. DocuSign provides a digital audit trail for the customer to track signing and lifetime access events. This Certificate of Completion is also tamper sealed upon download. This is so the Certificate of Completion cannot be modified after download, just like the document.

In both cases it is up to the viewer of the document to validate that the tamper seal is still intact.

All digital certificates support the following standards:

- X.509 PKI (Digital Certificate and Signature Technology)
- RFC 5280 – PKIX
- ISO 32000-1
- PAdES B-LTA
- ETSI EN 319 142
- FDA 21 CFR Part 11
- ETSI EN 319 411-1
- ETSI TS 102 023
- Adobe Approved Trust List

SOLICITATION # ITS-400335

e. Provides the ability for anyone to open a digitally signed PDF and observe a signature validity confirmation across the top of the file that indicates all signatures are signed and valid.

Yes, DocuSign places a signature validity confirmation at the top of each page of a signed document. Documents exported from DocuSign are digitally signed for tamper evidence. The tamper seal is an X.509 PKI standards based "Digital Signature" that is applied to the document at the time it is downloaded from DocuSign. The mechanism would indicate if the document has been changed since being downloaded. DocuSign provides a digital audit trail for the customer to track signing and lifetime access events. This Certificate of Completion is also tamper sealed upon download. This is so the Certificate of Completion cannot be modified after download, just like the document.

In both cases it is up to the viewer of the document to validate that the tamper seal is still intact.

f. Users of the e-signature service are given an opportunity to decline to use the service.

Yes, signers are presented with a Consumer Disclosure that is customizable using the State's legal language. Signers must accept disclosure in order to continue signing. If it is not accepted, the Signer can abandon the session or select to 'Decline to Sign' and will be presented with a text box to enter a reason. The Disclosure language accepted is audited and stored in the DocuSign 'Certificate of Completion' that accompanies every envelope transaction.

g. Does the solution provide the capability for electronic notarization.

Yes, DocuSign Electronic Notary feature provides this capability. The DocuSign electronic notary feature provides two primary functions:

- Allows Notaries to add their electronic notary credential information to their DocuSign account. All of the electronic notary signing sessions completed by the Notary using DocuSign are recorded in the Notary Journal.
- Allows senders to require that documents be notarized. The sender chooses the electronic Notary used in the signing process.

The use of electronic notary feature is currently limited to electronic Notaries registered in California, Florida, Idaho, Indiana, Kentucky, New Jersey, New York, North Carolina, Texas, and Washington. For more information please see <https://support.docusign.com/en/guides/ndse-user-guide-enotary-resources>.

h. Digital signature notifications are achievable through SMTP relay, direct email client integration (i.e. "mailto:"), or SMS (text messages). Please describe these and/or other capabilities.

As part of the SaaS platform, DocuSign sends emails to recipients based on the selected workflow. The emails contain web links with unique URLs. When users click on these web links, the default web browser is opened and the user starts the signing session.

i. Describe what notifications are sent to a user for signature?

DocuSign supports expirations and notifications/reminders. These settings are the default behavior for all documents sent from your account. You can choose to enforce these settings for all documents or allow users to modify the values for each document they send.

To allow users to change these values, select **Allow users to override these settings**.

Reminders

(Default: Off)

You can turn on reminders to send follow up emails to signers automatically. When you enable reminders, you specify when and how often to send notifications.

Expiration

By default, documents signing requests expire 120 days after sending. You can modify this value as desired. You can also add the option to send signers an expiration warning.

Best practice: Enter a low value for the option **Number of days to warn signers before expiration**, such as 3 days. Warning signers of an expiring envelope improves the likelihood of getting envelopes to complete, rather than expiring.

Expiration

Number of days before request expires:

Number of days to warn signers before expiration:

Allow users to override these settings

When a document expires, the status changes to Voided and it can no longer be viewed or signed by recipients. When an in-process document reaches five days to expiration, an expiration countdown appears under the document status in the Documents list.

4 Documents

Document Title	Status	Sort By
Purchase Requisition - Hsi 10/16/2014 To: Frank Hsi	Waiting for 1 Others Expires in 3 days	Recent Activity
Please DocuSign this document: Bill of Sale.pdf To: Becky Lee	Waiting for 1 Others on October 16, 2014	
Bill of Sale - Lee To: Annabelle User, Becky Lee	Waiting for 2 Others on October 16, 2014	
Please DocuSign this document: Bill of Sale - Ravetti To: Denise Ravetti, Fiona Lyon	Waiting for 2 Others on October 14, 2014	

e. Has expirations and notifications that can be set for a standard (e.g. three-month expiry) for whole organization, a division, and individual and etc.

Yes, DocuSign supports customizable expirations. By default, documents signing requests expire 120 days after sending. You can modify this value as desired. You can also add the option to send signers an expiration warning.

Best practice: Enter a low value for the option **Number of days to warn signers before expiration**, such as 3 days. Warning signers of an expiring envelope improves the likelihood of getting envelopes to complete, rather than expiring.

Expiration

Number of days before request expires: 50

Number of days to warn signers before expiration: 3

Allow users to override these settings

When a document expires, the status changes to Voided and it can no longer be viewed or signed by recipients.

When an in-process document reaches five days to expiration, an expiration countdown appears under the document status in the Documents list.

j. Please describe the solution's policy for handling customer's intellectual property, data, and information.

No DocuSign personnel can decrypt. DocuSign blobs are encrypted using a randomly assigned 256-bit key from the DocuSign Encryption Key Manager (DEKM). There are 1,000 active keys at any point in time. Keys in the DEKM are protected by a DB Master Key and an additional, Operations Master Key to enforce a form of key escrow –the full key requirements are escrowed in secure procedures. Additionally, each entry in the system is doubly encrypted. This encryption key management methodology is validated and tested by a qualified-third party audit firm and is annually reported upon with DocuSign's SSAE 16 report with no exceptions.

Upon access to an encrypted blob, the DEKM is queried to return the encryption key, decrypted by the DBA Master and still encrypted by the Operations Master. The Operations Master key is applied and the blob encryption key is applied to the blob to system. This methodology ensures a double-blind encryption key process where no single encryption key mechanism can be applied that would result in clear-text exposure.

k. Describe if the solution can import a predefined electronic list (i.e. CSV, ODBC, Excel) of customer's vendors and business partners. Please describe capability and any limitations that may exist.

A DocuSign Admin can easily upload a list of contacts using a properly formatted CSV file. This allows for the easy entering of the Signer(s) to a transaction.

11. Automation of Forms

Explain how the solution will address the automation of forms. Provide an explanation regarding the:

a. Process for integrating field validation (both data and format).

Data fields can be validated via predefined masks or by user defined regular expressions. With the use of a regular expression, it is possible to support any type of complex pattern validation.

b. Process for database integration.

DocuSign does not require or mandate the use of a database.

c. The limitations on the number of standard templates that can exist.

There are no limits on the number of templates that can be created within the system.

SOLICITATION # ITS-400335

d. Level at which standard templates exist – whole org., division, etc? Provide examples.

Templates can be created for use across any and all areas of the organization. The use of the templates is designated based upon User groups allowing you to specify who will have access to them. Examples of this would be HR templates. There may be HR templates that are only used by HR (such as employee policies, new-hire forms, etc.), there are also HR templates that may be used by other groups (such as Personnel action requests, time-off requests, etc.).

e. Revision process to forms without customization from vendor.

Users who have the appropriate permission level can make any necessary edits to the templates. This does not require any specific assistance from DocuSign resources. As always, the Users have access to DocuSign Support for assistance as well as a full line of courses for the use of DocuSign through DocuSign University. This can be accessed here:

<https://support.docusign.com/docusignuniversity>

f. Use of existing form templates created by other products.

The most common scenarios that we see are fillable PDF and Word documents. These have already been generated for use in form processing. DocuSign will not require Users to recreate the work that they have already completed. When uploading a fillable Word or PDF document, DocuSign reads the interactions within the document(s) and allows for the assignment of additional characteristics on those fields/tags (as DocuSign has additional features that Word/PDF do not have).

g. Methodology regarding how calculations are conducted within form.

Calculations are done via Formula tags. These tags provide the sender the ability to build a calculation using other tags in an envelope or template. The tags used in the formula are called "reference tags." The formulas built in a Formula tag can use the basic math operations of addition, subtraction, multiplication, division and rounding. The operators used in the formula are "+" (plus sign for addition), "-" (minus sign for subtraction), "*" (asterisk for multiplication), and "/" (forward slash for division).

h. Process for creating and publishing forms to agency websites.

DocuSign allow for the creation of templates that can predefine the signing order, messaging, settings, and tags that will be used when sending from a template. Upon creation of a template, you have the ability to create a self-service model for the publishing of the template to agency websites. These are called PowerForms and can be created directly from within the template in the DocuSign web console. The process is a simple step of creating the PowerForm from an action in the console. This will provide agencies with a URL (or embed code if preferred) to post as a link on the website as appropriate. There are no limits to how many templates can be provided as self-service forms.

i. Process required for citizens to use forms posted to Agency websites via the solution.

DocuSign provides the ability to use PowerForms. A traditional DocuSign envelope requires a sender to proactively send an envelope to a signer. PowerForms offer citizens a self-service option for embedding a reusable template into a third-party website via a DocuSign generated URL. In this way, signers can navigate to a portal and begin the envelope with no interaction from the sender. In addition to their flexibility, PowerForms feature the industry-leading DocuSign security and user-friendly experience that you and your customers expect.

How do PowerForms work?

- Step 1 Upload your document into DocuSign, and save the tags and workflow settings as a reusable template
- Step 2 Enable PowerForm usage on that template
- Step 3 Embed the PowerForm URL into your website, or send to signers, who can then fill out forms and sign documents on a self-serve basis

j. Methodology regarding how persons in a workflow can redline data in a form that is in process and route that form back to the originator for revision. Describe the form data capture – stored in form replica and/or recreated from database and ability to extract either way.

Though DocuSign does not provide a redlining feature, there are options around the needs for commenting and data changes.

Collaboration – Fields/Tags in DocuSign can be set to allow for the collaboration from Signers in the routing order. This provides the flexibility of making changes to data in the fields (as permission is granted). This can be set to require that it needs an initial of approval from the originator. Any time that changes are made to the fields, it is indicated in DocuSign.

Comments – This feature allows for the real-time communication of the Signer(s) in the routing order. Signer(s) can communicate within the transaction and all comments are tracked for historical purposes.

All data that is acquired in the DocuSign transaction is intelligent metadata that can be extracted by API calls and/or Connect push (automated push of data/documents via posted URL listener). Aside from documents, you can retrieve form field data contained in the documents (entered by signers, senders, or client systems), custom data fields with specific attributes provided by the sender or client systems (keys to foreign systems, account numbers, etc.), and transactional metadata to provide business intelligence into the usage of electronic signature (envelope status, recipient status, time sent, time signed, etc.).

k. Process for pre-populating user specific information such as name, address, and etc.

DocuSign has the ability to allow for integrated processes that amp data into the appropriate fields. Based off of web-service API calls, you can prepopulate data into a transaction (as well as initiate it) in order to avoid the need for data to be entered by a Signer. Data can also populate across the documentation in the appropriate areas based fields that ask the same question. For example, in a form asking for the recipient's phone number in multiple locations, you can easily setup DocuSign so that once the first instance of phone number is filled in, all subsequent phone number fields are automatically populated with the entered value.

l. Solution's method for marking sections of the document where signature is required.

As a part of the transaction process, DocuSign allows for the specification of the necessary signatures/interactions with the tagging capability. When a transaction is sent, tags are placed on the document by the Sender or automatically by the system via integration or anchor tags (auto-placement). User-placed tags are decided by the person sending the document(s). If auto-placement of tags is used or an integrated process, the signature tags are placed according to the rules set forth by the process, which will indicate the necessary points of signature (interaction).

m. Solution will allow forms to be labeled by type of process, such as HR, Finance, Payroll, etc.

DocuSign provides the ability to specify the transaction by envelope via Envelop Custom Fields. Envelope custom fields are used to classify, record, and track information about envelopes sent for signature. The sender enters field values when preparing an envelope. Envelope custom fields and their values are not shown to recipients.

The values for an envelope custom field can be free-text entries, or selected from a list of possible values. Envelope custom fields can be required or optional. Values are entered or selected when envelopes are created.

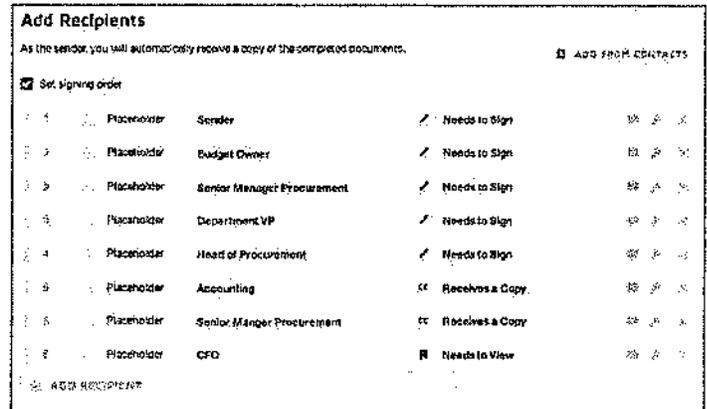
12. Workflow

Describe the solution's workflow capabilities. Include the functionalities below within the description:

a. Provide examples of templates for developing workflows per the solution that will standardize business engineering processes and improve workflow development efficiency.

DocuSign allows you to put powerful workflow creation tools in the hands of your business users.

- Route documents to your recipients in any order (e.g. **serial, parallel, or mixed**)
- Assign recipient-specific tasks including signing, viewing or copy receipt
- Utilize predefined documents, data and workflow, and route to signers and other recipients
- Enable signer self-service and list-based sending with PowerForms and Bulk Sending



With DocuSign's powerful signing workflows, the State can:

- ✓ Ensure the proper person acts on your documents at the right time
- ✓ Standardize processes, reduce preparation time, and enable end-to-end automation of your business
- ✓ Create and manage time-sensitive transactions

Ability to Change the Workflow

Some recipients can be set up in the template to manage the envelope recipients. Recipients can have the option to "Change Signer" or delegate the signing responsibility to someone else, and the process is defined for each template. Additionally, it is possible for the sender to "Correct" the workflow, and dynamically change a recipient's name or email address. Finally, it is possible to dynamically assign recipients through brokers. See "Agent Managed Envelopes" for more information. Note, DocuSign Admins and Senders have the complete control to enable or disable any of these features.

b. Any limitations to the size of documents sent through workflow.

- **Document limit:** A hard cap exists of less than 25MB per document.
- **Envelope limit:** No size limit exists on a per envelope basis (envelopes over a certain size may experience performance issues) - [Supported File Formats - New DocuSign Experience](#)

<https://support.docusign.com/en/articles/DocuSign-Document-and-Envelope-File-Size-Limitations>

c. Any limitations to the combined file size of a transaction with multiple files attached.

No, there is no limitation to the size of an envelope; however, we have seen some browsers on certain devices have performance issues with document packets that are gigabytes in size.

SOLICITATION # ITS-400335

d. Each person in the workflow is given the opportunity to review all documents, with a confirmation opportunity, before the transaction continues.

Yes, DocuSign supports serial workflows, meaning each person has to review and complete any assigned fields, including the ability to approve or decline, before the transaction continues to the next person.

e. The solution allows for rejection. If a form is rejected, specify how commenting, rerouting, markup of document is allowed.

Yes, signers have the ability to reject a form by selecting "Decline to Sign." The State has the ability to require a reason for declining to sign. The document is then routed back to the original sender.

f. The solution supports the approving/rejecting of multiple sections of a document by more than one approver and/or signer.

Yes, the sender can place multiple approve/deny tags in a single document.

g. Workflows are setup based on Roles and Permissions

Yes, access to workflows can be limited based on roles.

h. User initiates signing.

Yes, a user can initiate the signing process by uploading a document or using an existing template.

i. Each department/division/unit can have and maintain their own customizable workflows.

Yes, DocuSign supports templates for different departments, divisions, and units with customizable workflows. Users can be assigned to different permission groups to ensure they only have access to templates they need as part of their job duties.

j. Routing of multiple types of documents with multiple signatures within a single transaction.

Yes, The State can route multiple document types for signature by multiple parties in a single transaction. DocuSign does not limit the number of documents or signers that can be included in a single workflow.

k. Users can track the progress of a transaction – including stage and status.

Yes, users can track the progress of a transaction. Every envelope that you create or receive through DocuSign, has a status. The status indicates the current state of the transaction. Users can access the status of their transaction via the Management Tab in DocuSign. This list defines all the possible statuses:

- **Draft.** For an envelope, you created and then saved without sending.
- **Sent.** The email notification has been sent to at least one recipient. The envelope remains in this state until all recipients have viewed the document. (Shown in Reports and History only)
- **Delivered.** All recipients have viewed the document. (Shown in Reports and History only)

- **Waiting for Others.** The envelope has at least one recipient who has yet to complete their action. The recipient status in the Details view shows whether the outstanding recipients need to sign (Needs to Sign) or view (Needs to View). From the Manage page, you can see whose turn it is to sign by hovering over the status.
- **Needs to Sign.** You are a recipient and you need to sign.
- **Needs to View.** You are a certified delivery recipient and you are required to view the document.
- **Correcting.** The sender started to correct an in-process envelope and has not yet saved his changes. In this state, any outstanding signers are unable to view or sign. The sender must either save or cancel his changes to move the envelope out of the Correcting status.
- **Voided.** The sender canceled the envelope before it was completed. Recipients can no longer view or sign the document. Voided documents appear in your sending account as voided. You can still view and print the document, though it has a "VOID" watermark.
- **Declined.** A signer has declined to sign.
- **Completed.** An envelope is completed once all the recipients have completed their actions.
- **Expired.** A document that has exceeded its set expiration period without completing will expire. Recipients can no longer view or sign the expired document. Expired documents appear in your sending account as voided. You can still view and print the document, though it has a "VOID" watermark.
- **Delivery Failure.** The email notification did not reach the recipient. Review the [Details](#) to see which recipient status is listed as **Auto Responded**. For this recipient, check the email address you entered and correct the document to fix any errors. From the Manage page, you can see which recipient delivery failed by hovering over the status warning.

Waiting for Others

FILTERS Last 6 Months By Account Edit Search Quick View

Subject	Recipients	Last change	Folder
By questions for...	Melanie E. Deschutes, Sherman, Abby, e. Elisabeth Schreiber	2017 July 18 17:27	RESEND
Waiting for Others	Fred Marshall Status: 2017 July 18 14:50	2017 July 18 14:50	RESEND

Sent

DELIVERY FAILURE

Brad Malion
Email Sourced

Recipients

Last change

2017 July 19 13:55

CORRECT

- **Authentication Failed.** At least one signer has failed the authentication check. You can either send a reminder to the recipients, which gives the signer another chance to access and pass the authentication. Or you can correct the envelope and modify the authentication setting. The envelope History provides additional detail on the authentication failure.

l. The process for copying previously created workflows

DocuSign allows for the use of multiple workflows with the system. These are easily generated within templated processes that are created/maintained by the appropriate people with the given permission levels. Typically, the recommended process is to create the workflows within the Sandbox (test) environment for appropriate testing and then moving them over to Production. This is an easy process of downloading the templated process and then simply uploading into Production.

m. The solution generates a diagram of the workflow.

Yes, senders can view a graphical representation of the workflow by selecting the Order Diagram link within each template and envelope.

Signing Order Diagram



When a user sends a transaction (one or more documents) for signature, they can set the routing in order to determine the specific order that the transaction needs to go through. If this is done on an ad hoc basis, the workflow will not be saved, but the user can clone a previous workflow if needed. For more consistently used documentation, templates can be created and managed locally by users who have the permissions to do so. This will allow for the setting of a specific user(s) and or groups for signing at defined times within the workflow.

n. User can abandon signing a document.

Yes, signers can select an option to "Finish Later." The signer can then return later to complete the transaction.

o. Portions of the workflow that are configurable by the Department/Division/Unit.

Yes, workflows are configurable by different departments/divisions/units.

p. Queues are established to assist users to process, review, analyze and approve depending on role.

DocuSign provides several different methods to locate documents/transactions that may require action. This can be seen when the User logs into the web console and/or mobile app and is taken to the Home Screen with quick views.

Quick views are a great way to easily filter documents for key categories. When a user selects a Quick View, the results list shows all of the documents that match the selected category. These are results are restricted to document activity from the last six months. To get different results, use the Filters menu to select a different time frame or specify the sender, or enter a search term to narrow the quick view results by document name, recipient name, recipient email, or envelope ID. The quick view options are:

- Action Required - Documents awaiting your action, which you need to either sign or view.
- Waiting for Others - Documents sent by you that are waiting for others to act on, either to sign or to view.
- Expiring Soon - In process documents that are due to expire within six days.
- Completed - Documents with the status Completed, either sent or received.

q. Support Ad Hoc signing from cloud and smart devices.

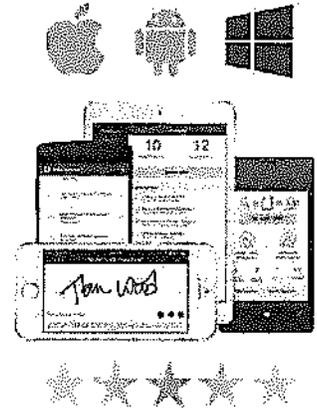
Yes, DocuSign supports Ad Hoc signing from cloud and smart devices. DocuSign is specifically engineered and tested to work for signers on regardless of device type. It recognizes the device and may alter the HTML-5 rendered interface

SOLICITATION # ITS-400335

accordingly for the device being used to sign the document. We currently support signing on all HTML-5 capable browsers and mobile devices. Additionally, DocuSign is the only platform that offers native mobile apps for all major platforms: iOS (iPad/iPhone) and Android. DocuSign is available through the Blackberry mobile browser but is not available through a native Blackberry mobile application.

Access your DocuSign account directly from your computer or your mobile device. Sign documents, send documents out for signature, gather signatures in-person, monitor document status, access completed documents and much more. Whether you are in the office, at home, or on-the-go – DocuSign works every time from every device. Additionally, you can access from mobile browsers as well as from our native Apps.

- Support BYOD with native apps for all major platforms
- Quickly sign and send documents from the road—even without an internet connection
- Automate signature workflows into your company’s mobile app with the DocuSign Mobile Client Library
- Meet the highest mobile device management standards
- Receive instant transaction updates
- Apps available for iOS and Android.



With DocuSign’s mobile apps:

- Sign and send documents from anywhere
- Easily manage your documents, including void and remind
- Real-time status updates provide instant visibility

Offline Mobile capabilities –DocuSign is the only vendor to enable the following from a mobile device when the mobile device does not have internet access:

- In-person Signing
- Create Envelope
- Add Document
- Add In-person Signer
- Add Remote Signer
- Local Document Storage
- Enable Offline Mode

r. *Workflow creation can be automated. (i.e. – Roles copied from other systems such as HR/Payroll systems).*

DocuSign allows the ability to define permission sets which can be mapped to a role. There is no guarantee that roles from other systems can be mapped 1:1 with roles in DocuSign. We would need to understand your requirements more fully to be able to provide a comprehensive answer. DocuSign allows the ability to define permission sets which can be mapped to a role. There is no guarantee though that roles from other systems could be mapped 1:1 with roles in DocuSign. We would need to understand your requirements more fully to be able to provide a comprehensive answer.

s. *Documents which do not require signature are bound to signature documents and routed through the workflow.*

Yes, documents that do not require signature can be added into an envelope to be reviewed by signers. In addition, the State can place tags requiring a signer to approve/reject documents in order to confirm the signer reviewed the document.

t. Workflow can be redirected and users injected to the flow:

Yes, users can be added to the workflow until it has been completed.

u. Support branding and color scheme customization of document packages for signature.

Yes, DocuSign supports branding customization. DocuSign is easily customizable and configurable. One method of customization is by branding. Branding your DocuSign account is an excellent way to add the look and feel of your organization's brand to the sending, signing, and email process making it easier for users to identify envelopes coming from your organization. The DocuSign Account Custom Branding feature lets you set the colors, logo, and text for your account to enhance the sending and signing experience. You can create any number of brand profiles with different settings to reflect each of your corporate brands or different internal divisions or departments.

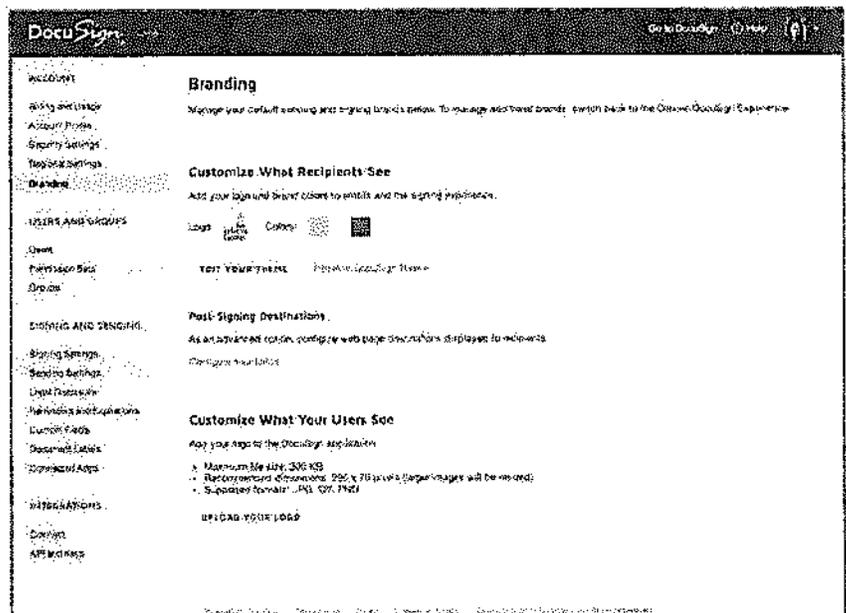
When you create or change a branding profile, it applies to everyone using that profile and affects all envelopes sent with that profile.

Another approach to customization is using the DocuSign API's. Each function is available programmatically, allowing the customer to create a unique experience, including embedding DocuSign in a custom application (mobile or web-based).

DocuSign is also highly configurable, allowing the customer to create reusable templates, define workflows, save personal reports, for example, without required service from DocuSign. Each DocuSign customer has unique requirements and DocuSign has been designed to be flexible to meet those requirements.

Email Branding

Emails can be customized with the subscriber's logo and color scheme. The email subject and email message can also be customized.



A unique capability of DocuSign is that each recipient in a multi-recipient workflow can receive an individualized email, with different verbiage. In a multi-language scenario, each recipient may also receive a different, localized set of emails. Not only is the UI localized, but the email body itself.

v. Support document creator workflow rerouting with and without workflow start over.

The solution provides the ability to be an individual workflow or be a part of a larger workflow that takes place before and/or after the DocuSign process. Most commonly, this is done with documentation that is created and/or edited prior to the need for the eSignature process. Upon the initiation of the DocuSign process, it is a fully tracked and audited process that would require restart if changes are needed to the document(s). If there are changes needed around the signing steps and or additional documentation to be added, a simple Correct feature could be used, which does not require that the transaction be restarted.

w. How an external system process can be added as a workflow step/approval.

Generally speaking, the process of satisfying a DocuSign workflow step is designed to be an interactive, human step. However, some customers support systematic interactions of Recipient workflow steps through creative solutioning. The basic process is:

1. Include a step for the system process in the Recipient Workflow. This Recipient will need a name and email, but no human user is expected to monitor the email. For the sake of this description, the Recipient will be named "System Pause".
2. You can programmatically detect when the workflow reaches the System Pause Recipient. At this point, your system process can perform its function.
3. When the system process is complete, if the intent is to approve the step so that the workflow continues forward, you remove the System Pause Recipient from the workflow through the API. This has the effect of moving the workflow to the next step in the process, including the option of completing altogether. If the outcome of the system process is to not approve the step, you can programmatically Void the transaction, bringing it to a halt.

x. Describe how the solution will generate workflow and forms meta-data and the content of such meta-data specifying what is included, and what is excluded.

All aspects of each transaction are fully logged (including name, email address, IP address, date/time, authentication, and activity) and captured in a detailed transaction history which is stored in perpetuity as hashed and encrypted data within the DocuSign system. This data is available on demand from the DocuSign system and may also be programmatically exported to client systems in real-time as transactions progress to a completed state. In addition, DocuSign also generates a Certificate of Completion for every transaction in the form of a digitally signed PDF document which is designed to be a court admissible document.

Audit trails, such as signatures and documents, are always stored in encrypted form using an x.509 certificate. A hash is also taken before each change, and compared to previous SHA-2 hash values to ensure the document has not been modified. After any change, a new hash is taken and stored physically and logically separate from the document.

DocuSign tracks activities at both a User and Transaction (Envelope) level. This is relevant both to an auditing perspective as well as driving the workflows around the document being signed. All the audit activities listed below are available to the Sending party through the user interface or programmatic API.

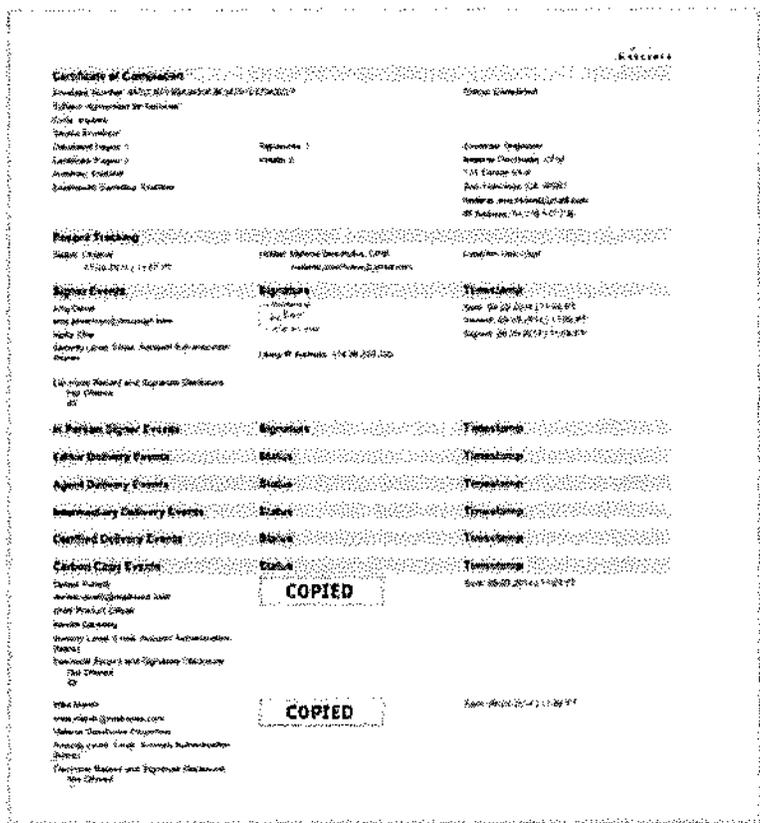
From the standpoint of a Signing User, DocuSign audits the following events:

SOLICITATION # ITS-400335

- When a User was invited to sign, including whether the invitation was successfully delivered
- When a User passed (or failed) various authentication steps that were required to access the documents
- When a User agreed to a Consumer Disclosure consent
- When a User first viewed the documents
- When a User signed their documents
- Anytime a User downloaded the documents
- Anytime a User viewed the documents
- When a User declines to sign the documents
- Anytime a User marks-up a document or provides data values

From the standpoint of the Sender, DocuSign audits the following events:

- When the sender initiated the Envelope
- When the sender activated the Envelope for signature
- Anytime the sender modifies the Envelope contents or signature workflow
- Anytime the sender downloads the documents
- Anytime the sender views the documents
- When a sender voids the Envelope (revoke the ability to eSign)



From the standpoint of a Transaction: DocuSign audits the following events:

- When the Envelope was initiated
- When the Envelope was activated for signature
- When the Envelope was viewed by all parties
- When the Envelope was signed by all parties
- When the Envelope was completed
- When the Documents were deleted
- When the physical location of the electronic Envelope was transferred to another electronic vault

13. Signature/Initialing

Describe the solution's signature and initialing capabilities. Include how the:

- Digital signature is linked to the documents being signed. Describe how this is achieved.

Yes, documents exported from DocuSign are digitally signed for tamper evidence. The tamper seal is an X.509 PKI standards based "Digital Signature" that is applied to the document at the time it is downloaded from DocuSign. The mechanism would indicate if the document has been changed since being downloaded. DocuSign provides a digital audit trail for the customer to track signing and lifetime access events. This Certificate of Completion is also tamper sealed upon download. This is so the Certificate of Completion cannot be modified after download, just like the document.

b. Solution assigns and restricts the sole control of the signature to the owner.

For external signers, Yes. DocuSign supports a variety of authentication methods to ensure the person signing is in sole control of their signature. In addition to standard email address authentication, DocuSign offers an industry-leading choice of authentication services for customers, partners and developers. By default, authentication is at the point of signing, making it a seamless process that keeps business digital.

- **Email Address.** Requires access to a specific email address before access is granted.
- **Access Code.** Requires the signer to provide a sender-generated code shared out of band, usually over the phone. The signer must enter the code to open the document.
- **SMS.** A two-factor solution that requires the signer to provide a randomly-generated one-time passcode sent via SMS text message to the signer's mobile phone to open the document.
- **Federated Identity/Single Sign-On.** Federated Identity validates authentication by an external system integrated with DocuSign via the industry-standard protocol SAML.
- **Third-party.** Validates the signer's Salesforce, Google, Yahoo!, or Microsoft account credentials, with additional options for social network credentials from Facebook, Twitter, and LinkedIn.
- **DocuSign Credentials.** Validates a recipient's existing DocuSign account associated with a username and password.
- **ID Check.** This third-party service by LexisNexis validates a signer using a KBA (knowledge-based authentication) process. The signer must correctly answer a list of personally identifying questions to open the document (OFAC Checking and Age Verification can be part of this).
- **Two-Factor Phone Authentication.** This third-party service by Authentify validates a signer's access to a phone number and predetermined access code for entry. The signer's spoken name is also recorded as a biometric print.
- **Digital Certificates** - DocuSign offers digital certificates as part of its Standards-Based Signatures platform. Using digital certificates during signing provides higher levels of identity authentication and document transaction security. Further explanation of DocuSign's Standards Based Signatures can be found here: <https://www.docusign.com/sites/default/files/standards-based-digital-signatures.pdf>

- ✓ Increased legal enforceability
- ✓ Ensures the highest level of data privacy
- ✓ Meets authentication regulations and best practices (e.g. FFIEC and CSA recommendations)
- ✓ Supports access control requirements for security certifications including ISO 27001

For users within NCID, DocuSign's OAuth supports the standard grant types for web and smart applications. This allows third-party integrations to authenticate a user without prompting the user for their password. In addition, this model of authentication allows DocuSign to introduce new authentication features without having to update any third-party integrations. DocuSign SSO currently supports the following SAML protocols, OASIS SAML 2.x or 1.x with HTTP POST binding or earlier.

c. Solution captures the users "actual" signature and initials.

Yes, DocuSign currently provides several means to create a Signature, including:

- Adoption of a pre-generated signature and GUID
- Handwriting capture via mobile or touchscreen device
- Uploaded sample of handwriting via scanner or mobile camera

d. Solution captures a picture of the signature owner and associates it with the actual signature.

DocuSign provides the ability to require attachments to the transaction. This would allow for the inclusion of a required attachment to take a picture of the Signer as he/she handles their step in the process.

e. Solution captures speed, pressure and x-y coordinates of signatures.

DocuSign does not capture the speed, pressure, or x-y coordinates of a signature; however, the location of the signature is defined by defined tags for signature/initial. This provides the Signer(s) with the appropriate placement of their signature(s).

To comply with the eSign act of 2000, DocuSign provides a digital audit trail for the customer to track signing and lifetime access events. A formal Certificate of Completion is created upon signature of all document parties. This contains the non-repudiation information for legality of the applied electronic signature.

f. Receiver of data can determine origin.

The digital audit trail tracks when a signer views and signs, captured data/time/IP address for each signer. This allows for the tracking of which person/persons conducted the interactions to enter data and/or sign the document(s).

g. Electronic document cannot be altered without detection at any time after being signed.

Yes, documents exported from DocuSign are digitally signed for tamper evidence. The tamper seal is an X.509 PKI standards based "Digital Signature" that is applied to the document at the time it is downloaded from DocuSign. The mechanism would indicate if the document has been changed since being downloaded. DocuSign provides a digital audit trail for the customer to track signing and lifetime access events. This Certificate of Completion is also tamper sealed upon download. This is so the Certificate of Completion cannot be modified after download, just like the document.

h. Code or other mechanism is used to create digital signatures and how that code or mechanism is unique to that individual at the time of signature.

- DocuSign can support both electronic and digital signatures.
- With electronic signatures, there can be multiple signers in a transaction and there is a single digital signature that is used to seal the signed documents from tampering.
- When using digital signatures, a digital signature is specifically applied to each transaction participant upon signing.
- We support advanced functionality in electronic and digital signatures. For specifics on the advanced functions and how they apply to the State's situation, we require a better understanding of your requirements.

DocuSign can support both electronic and digital signatures. With electronic signatures, there can be multiple signers in a transaction and there is a single digital signature that is used to seal the signed documents from tampering. When using digital signatures, a digital signature is specifically applied for each transaction participant upon signing. We support a lot of advanced functionality when it comes to signing and for us to know how we map to your needs would require a better understanding of your requirements. DocuSign combines the digital and electronic signature product in one cloud based solution.

- o A digital signature, using an x.509 certificate which is unique to the signer, is dynamically provisioned.
- o The document is "hashed" and this hash is digitally signed.
- o If multiple signers are involved then each will digitally sign, whether they are internal users or external signers who are signing for the first time.
- o Digital Signatures happen transparently, as easy as signing electronically.

SOLICITATION # ITS-400335

o In addition, the electronic signature is also signed by the platform, servicing as a "witness" to the transaction and applying a final digital certificate around the entire set of signer digital signatures, to authenticate it originated from DocuSign and to prove document integrity.

DocuSign gives your transaction the best chance of having legal force and effect and business force and effect, regardless of where in the world, your transaction or signature needs to be relied upon. Below are the standards that DocuSign meets:

- o X.509 PKI (Digital Certificate and Signature Technology)
- o RFC 5280 – PKIX
- o ISO 32000-1
- o PAdES B-LTA
- o ETSI EN 319 142
- o FDA 21 CFR Part 11
- o ETSI EN 319 411-1
- o ETSI TS 102 023
- o **Adobe Approved Trust List**
- o ETSI EN 319 411-2 – EU QCP
- o EU Trusted List Service Provider (TSL)

Also included in the artifacts returned after signing is the "Certificate of Completion", which is also digitally signed. It provides:

- o Evidence of compliance with eSign law (in addition to the digital compliance)
- o Exactly how each signature was authenticated
- o Evidence, such as IP address, timestamp, email, geolocation, and other info

14. Repudiation

Describe how the solution addresses repudiation; specifically address how the solution will provide:

a. True and correct copy of document received – provide sufficient evidence to show how the copy of record was derived from and accurately reflects the electronic document as it was received by the system, this evidence is also necessary to establish document integrity.

Yes, All aspects of each transaction are fully logged (including name, email address, IP address, date/time, authentication, and activity) and captured in a detailed transaction history which is stored in perpetuity as hashed and encrypted data within the DocuSign system. This data is available on demand from the DocuSign system and may also be programmatically exported to client systems in real-time as transactions progress to a completed state. In addition, DocuSign also generates a Certificate of Completion for every transaction in the form of a digitally signed PDF document which is designed to be a court admissible document.

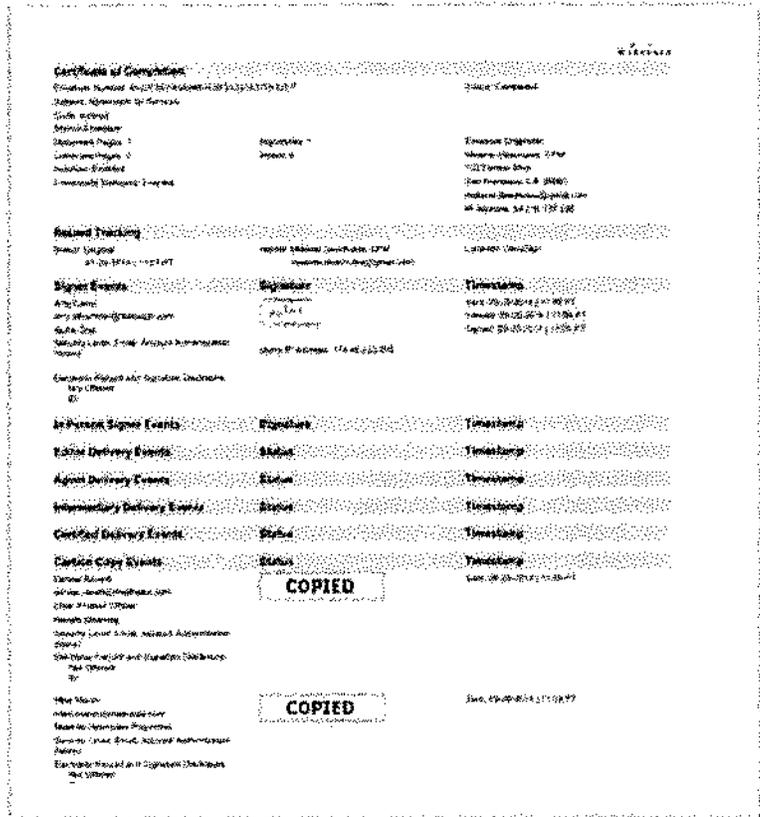
Audit trails, such as signatures and documents, are always stored in encrypted form using an x.509 certificate. A hash is also taken before each change, and compared to previous SHA-2 hash values to ensure the document has not been modified. After any change, a new hash is taken and stored physically and logically separate from the document.

DocuSign tracks activities at both a User and Transaction (Envelope) level. This is relevant both to an auditing perspective as well as driving the workflows around the document being signed. All the audit activities listed below are available to the Sending party through the user interface or programmatic API.

SOLICITATION # ITS-400335

From the standpoint of a Signing User, DocuSign audits the following events:

- When a User was invited to sign, including whether the invitation was successfully delivered
- When a User passed (or failed) various authentication steps that were required to access the documents
- When a User agreed to a Consumer Disclosure consent
- When a User first viewed the documents
- When a User signed their documents
- Anytime a User downloaded the documents
- Anytime a User viewed the documents
- When a User declines to sign the documents
- Anytime a User marks-up a document or provides data values



From the standpoint of the Sender, DocuSign audits the following events:

- When the sender initiated the Envelope
- When the sender activated the Envelope for signature
- Anytime the sender modifies the Envelope contents or signature workflow
- Anytime the sender downloads the documents
- Anytime the sender views the documents
- When a sender voids the Envelope (revoke the ability to eSign)

From the standpoint of a Transaction: DocuSign audits the following events:

- When the Envelope was initiated
- When the Envelope was activated for signature
- When the Envelope was viewed by all parties
- When the Envelope was signed by all parties
- When the Envelope was completed
- When the Documents were deleted
- When the physical location of the electronic Envelope was transferred to another electronic vault

b. A human-readable format that clearly and accurately associates all the information provided in electronic document with descriptions or labeling of the information and provides the opportunity to repudiate the electronic document based on this review.

Yes, DocuSign generates a Certificate of Completion for every transaction in the form of a digitally signed PDF document which is designed to be a court admissible document.

SOLICITATION # ITS-400335

c. Inclusion of other information necessary to record meaning of document – such as data field labels, signatory information such as references to validation mechanism, and transmission source information.

When sending the transaction, Senders can set additional details around the document labels, details, and envelope custom information.

Fields can have additional Data Label names placed on them. The service also allows the configuration of Envelope Custom Fields which can be used to associate particular values or text with a document for ease of searching (i.e. a form number, applicant name, etc.).

Transmission details as well as all Signer details are held within the tracking audit history and Certificate of Completion.

d. Procedures to address submitter/signatory repudiation of a copy of record.

DocuSign provides a digital audit trail for the customer to track signing and lifetime access events. A formal Certificate of Completion is created upon signature of all document parties.

All documents exported from DocuSign are digitally signed for the purpose of tamper evidence. The tamper seal is an X.509 PKI standards based "Digital Signature" that is applied to the document at the time it is downloaded from DocuSign. The mechanism would indicate if the document has been changed since being downloaded. DocuSign provides a digital audit trail for the customer to track signing and lifetime access events. This Certificate of Completion is also tamper sealed upon download. This is so the Certificate of Completion cannot be modified after download, just like the document.

Regarding repudiation, DocuSign sets the standard for world-class legal protection. With presence in 188 countries, you can trust DocuSign meets statutes and regulations around the world, and leads the industry in compliance and enforceability. We provide the most authentication options, a comprehensive digital audit trail and carrier-grade security.

DocuSign was the first company to warrant compliance with the U.S. E-SIGN Act, state laws modeled after 1999 UETA and certain key aspects of the UK Electronic Communication Act (2000). DocuSign is designed for global compliance with key components of the European Directive 1999/93 EC on a Community Framework for Electronic Signatures, including the UK Electronic Communication Act. DocuSign fully enforces consumer consent, unique signature adoption and signature process flow provisions. DocuSign meets specialized rules from the FDA, FTC, FHA, IRS, FINRA, among many others. We provide extensive, configurable authentication options to verify the identities of your signers.

DocuSign will go to court with you. While DocuSign has a successful history of providing customers with all the evidence they need to defend their documents against repudiation, DocuSign is available to assist our customers with legal challenges by testifying in court to support the validity of DocuSigned documents.

e. Confirmation of receipt of intact form data or record.

Confirmation notifications can be provided as per API calls. There are abilities to also notify the appropriate people if there are any errors on the data transfer.

f. Expunging of transaction upon authorized request.

There are several methods to request a purge from customer perspective - with a retention policy ("Document Retention" feature), via the API (PurgeDocuments method), or manually. The "Document Retention" feature in DocuSign will purge documents from the DocuSign servers (for Completed, Declined, and Voided envelopes) N days after the envelope becomes Completed/Declined/Voided, where N is the number you specify in Preferences > Features > Document Retention (link). The envelope documents are placed in a purge queue for deletion in 14 days. A warning email notification is sent to the sender and

SOLICITATION # ITS-400335

recipients associated with the envelope notifying them that the envelope document will be deleted in 14 days and providing a link to the documents. Another email is sent 7 days later with the same message. At the end of the 14-day period, the envelope documents are deleted from the system. Envelopes where documents are purged retain envelope data (audit trail, certificate of completion, etc.) An envelope can also be manually deleted from the console but it must be completed or voided. It is moved to a deleted folder and then on a daily basis permanently removed.

Document Deletion can occur directly from the web application by selecting the delete option for a specific envelope or dragging it into the Deleted folder. When an envelope is dragged into the Deleted folder, a Delete job runs at 9pm that evening, removing the pointer of the user who deleted the envelope. If no pointers are left, the envelope docs are immediately purged (meaning the envelope no longer resides in any DocuSign user folder).

g. Long term validation of electronically signed document. Describe how electronically signed document will maintain validity for long term (multiple years out).

DocuSign tracks all aspects of each transaction and are fully logged (including name, email address, IP address, date/time, authentication, and activity) and captured in a detailed transaction history which is stored in perpetuity as hashed and encrypted data within the DocuSign system. This data is available on demand from the DocuSign system and may also be programmatically exported to client systems in real-time as transactions progress to completed state. In addition, DocuSign also generates a Certificate of Completion for every transaction in the form of a digitally signed PDF document which is designed to be a court admissible document.

15. Notification

Describe the solution's notification capabilities, include if the solution:

a. Provides opportunity to review certification statements and warnings (including any applicable certifications that false certification carries criminal penalties).

Yes, signers are presented with a Consumer Disclosure that is customizable using the State's legal language. Signers must accept disclosure in order to continue signing. If it is not accepted, the Signer can abandon the session or select to 'Decline to Sign' and will be presented with a text box to enter a reason. The Disclosure language accepted is audited and stored in the DocuSign 'Certificate of Completion' that accompanies every envelope transaction.

b. Provides notification that copy of record is available and this notification is configurable by each Department/Division/Unit.

Yes, users in the signing workflow will receive a notification when the signing process is complete. User download is an option available to all recipients during a DocuSign signing session.

Email attachment is available if enabled by the sending organization. By default, DocuSign sends a completion notification email to all recipients when the entire workflow is complete, which contains a secure link to the completed documents. Sending organization can elect to enable a feature which will attach a pdf of the completed document(s) and/or the Certificate of Completion.

c. Flags accidental submissions.

When a Signer interacts with a transaction, everything is tracked in the process to be a part of the audit history as well as the Certificate of Completion. If a signer decides to 'Decline to Sign,' DocuSign will indicate the decline as well as require a reason that is held in the transaction history.

SOLICITATION # ITS-400335

If a citizen initiates a transaction (via PowerForm) and then decides that it was accidental, they can void the transaction, which is tracked. DocuSign can also allow for settings around the expiration of transactions. This will void the open transactions after the designated timeframe. All of these transactions can be searched upon as well as scheduled in reporting within the web console.

d. Supports setting expirations and notifications.

Yes, DocuSign supports expirations and notifications/reminders. These settings are the default behavior for all documents sent from your account. You can choose to enforce these settings for all documents or allow users to modify the values for each document they send.

To allow users to change these values, select **Allow users to override these settings**.

Reminders

(Default: Off)

You can turn on reminders to send follow up emails to signers automatically. When you enable reminders, you specify when and how often to send notifications.

Expiration

By default, documents signing requests expire 120 days after sending. You can modify this value as desired. You can also add the option to send signers an expiration warning.

Best practice: Enter a low value for the option **Number of days to warn signers before expiration**, such as 3 days. Warning signers of an expiring envelope improves the likelihood of getting envelopes to complete, rather than expiring.

Expiration

Number of days before request expires:

Number of days to warn signers before expiration:

Allow users to override these settings

When a document expires, the status changes to Voided and it can no longer be viewed or signed by recipients.

When an in-process document reaches five days to expiration, an expiration countdown appears under the document status in the Documents list.

4 Documents

	Sort By	Recent Activity
<p>Purchase Requisition - HSI 10/16/2014 To: Frank HSI</p>	<p>Waiting for 1 Others Expires in 3 days</p>	<p>REMIN</p>
<p>Please DocuSign this document: Bill of Sale.pdf To: Becky Lee</p>	<p>Waiting for 1 Others on October 16, 2014</p>	<p>REMIN</p>
<p>Bill of Sale - Lee To: Annabeta User, Becky Lee</p>	<p>Waiting for 2 Others on October 16, 2014</p>	<p>REMIN</p>
<p>Please DocuSign this document: Bill of Sale - Ravotti To: Garise Ravotti, Fiona Lyon</p>	<p>Waiting for 2 Others on October 14, 2014</p>	<p>REMIN</p>

e. Has expirations and notifications that can be set for a standard (e.g. three-month expiry) for whole organization, a division, and individual and etc.

Yes, DocuSign supports customizable expirations. By default, documents signing requests expire 120 days after sending. You can modify this value as desired. You can also add the option to send signers an expiration warning.

Best practice: Enter a low value for the option **Number of days to warn signers before expiration**, such as 3 days. Warning signers of an expiring envelope improves the likelihood of getting envelopes to complete, rather than expiring.

Expiration

Number of days before request expires: 50

Number of days to warn signers before expiration: 3

Allow users to override these settings

When a document expires, the status changes to **Voided** and it can no longer be viewed or signed by recipients.

When an in-process document reaches five days to expiration, an expiration countdown appears under the document status in the Documents list.

f. Makes it clear that the signed document represents a completed declaration of will, and not just a draft which the signatory did not intend to be bound by -- Finality function.

Yes, signers are presented with a Consumer Disclosure that is customizable using the State's legal language. Signers must accept disclosure in order to continue signing. If it is not accepted, the Signer can abandon the session or select to 'Decline to Sign' and will be presented with a text box to enter a reason. The Disclosure language accepted is audited and stored in the DocuSign 'Certificate of Completion' that accompanies every envelope transaction.

g. Makes a signatory aware that by his/her signature he/she is entering into a binding transaction -- Cautionary function.

Yes, signers are presented with a Consumer Disclosure that is customizable using the State's legal language. Signers must accept disclosure in order to continue signing. If it is not accepted, the Signer can abandon the session or select to 'Decline to

Sign' and will be presented with a text box to enter a reason. The Disclosure language accepted is audited and stored in the DocuSign 'Certificate of Completion' that accompanies every envelope transaction.

h. Includes automatic acknowledgement of receipt.

There are multiple ways in which DocuSign provides and tracks notifications to the Signer(s). All actions that happen in the routing order are tracked, which can include the people who are entered as a Carbon Copy (CC) as well as a Needs to View (which requires that they open and view the transaction document(s)). In the tracking history of the transaction, every action is tracked which indicates everyone who has received the transaction, whether needing to interact or not.

16. Storage

Describe the following storage capabilities; include if the solutions storage functionality can:

a. To print or store locally by person(s) in the process.

Yes, all users involved in the signing ceremony have the ability to print or download the contents of the envelope.

b. Form data or record will be stored – vendor or agency.

Yes, form and record data are stored. The document retention policy is configurable by the client. Most clients leave signed documents in the DocuSign system indefinitely to retain an independent third party that can warrant the documents have been securely stored and have not been altered. It is also common for clients to utilize the DocuSign Connect publisher service to deposit copies of signed documents in their integral document repositories and applications so that a local copy is kept behind their firewall and readily accessible. However, DocuSign supports the unique retention policies of each of its clients by enabling them to remove documents from the system as well. This can be performed on a policy-basis according to a pre-defined schedule (ex: 14 days after completion); or it can be performed on the explicit basis upon instructions from a client system. In either of these cases, DocuSign will remove the documents from the system, though it will maintain the audit log so that it can vouch for the execution history of the documents.

c. Provide costs estimate for vendor storage in Section IV. Provide cost estimate for any transmission cost if stored at agency in Section IV.

DocuSign includes unlimited Cloud storage for all documents routed with DocuSign at no additional cost to the DocuSign License.

d. Store and accommodate according to each department/division/unit record retention and disposition schedule.

Yes, the document retention policy is configurable by the client. Most clients leave signed documents in the DocuSign system indefinitely to retain an independent third party that can warrant the documents have been securely stored and have not been altered. It is also common for clients to utilize the DocuSign Connect publisher service to deposit copies of signed documents in their integral document repositories and applications so that a local copy is kept behind their firewall and readily accessible. However, DocuSign supports the unique retention policies of each of its clients by enabling them to remove documents from the system as well. This can be performed on a policy-basis according to a pre-defined schedule (ex: 14 days after completion); or it can be performed on explicit basis upon instructions from a client system. In either of these cases, DocuSign will remove the documents from the system, though it will maintain the audit log so that it can vouch for the execution history of the documents.

e. Allow procedures for retrieving documents from Vendor; during contract term.

Yes, it is common for clients to utilize the DocuSign Connect publisher service to deposit copies of signed documents in their integral document repositories and applications so that a local copy is kept behind their firewall and readily accessible.

SOLICITATION # ITS-400335

The DocuSign storage repository is updated automatically as envelopes are routed and signed. Using DocuSign API, it is possible to download from the repository. You access the envelopes stored with DocuSign via either the DocuSign Console, DocuSign Retrieve, or potentially a DocuSign API integration.

f. *Allow procedures for retrieving documents from Vendor; expired contract term.*

Yes, customers have 90 days to retrieve any documents after contract expiration.

g. *Format documents are received and stored in.*

All documents are saved and stored as PDF files.

h. *Support document package labeling for ease of segmented document storage outside of the native solution data center*

DocuSign provides document filing as part of our System of Agreement functionality. All transactions are stored in our service indefinitely unless a customer chooses to set a retention policy and are accessible from the account that initiated the transaction.

For scenarios in which the Documentation, data, etc. is to be stored in other system(s), the service also allows the configuration of Envelope Custom Fields which can be used to associate particular values or text with a document for ease of searching (i.e. a form number, applicant name, etc.).

i. *Process for retrieving information required to meet eDiscovery requests when documents are stored at a Vendor operated or controlled site; or when information retrieval requires participation of the Vendor or a third party.*

To fully research across the data and documentation in DocuSign, it is best to extract the data and details to an internal system for full eDiscovery. DocuSign offers multiple options for customers to extract completed documents, the Certificate of Completion, transaction metadata and document data.

The DocuSign API (available in REST and SOAP) provides you with a powerful, convenient, and simple Web services API for interacting with DocuSign.

DocuSign Connect is a push service that sends real-time envelope and recipient data updates to customer listener applications. These updates are generated by changes to the envelope as it progresses from sending to completion. Connect provides updated information about the status of these transactions, including the actual content of document form fields. Connect is useful to organizations that want a real-time view into the transactions across their user base in a centralized location. This information can be customized to drive reporting or workflow specific to that organization's needs. Customers can create multiple Connect configurations, each with different events or users, and set up different listeners to monitor those configurations.

DocuSign Retrieve is a windows-based tool that "retrieves" envelopes, documents, and data from DocuSign for use in external systems, using the DocuSign API. Retrieve runs on your system and can be run as one-time request or on a schedule. When run, Retrieve contacts DocuSign, and retrieves envelopes, documents, and information for those envelopes based on filters you set. DocuSign Retrieve requires additional licensing.

DocuSign Total Search – new feature

DocuSign's Total Search feature is described below and is not included in our pricing, since it is a new optional feature. We are happy to provide providing and additional information if requested.

SOLICITATION # ITS-400335

DocuSign Total Search (powered by Seal) is designed to drive 'human discovery': it will enable customers to centralize all of their digital agreements, organize them using metadata (structural data), and search inside them using natural language terms (unstructured data). DocuSign Intelligent Insights (powered by Seal) is designed to drive 'machine discovery': it will use artificial intelligence and machine learning to automatically extract mission critical legal concepts like indemnification, warranty and most favored nation, among others. DocuSign Compliance Packs (powered by Seal) use the same artificial intelligence and machine learning to extract concepts derived from key regulations, including GDPR.

These integrated platform extensions from Seal, available later this year, bring powerful new capabilities to the 'manage' stage of modern Systems of Agreement. Customers can instantly and easily find agreements, regardless of their origin or storage location. They can then compare sections of similar agreements to identify inconsistent contracted terms, areas of exposure, and potential revenue leakage. And they can review auto-extracted terms and concepts to ensure compliance and minimize exposure to risk.

j. Process for searching and sorting information stored at Agency site to meet eDiscovery requests (e.g. – record identifiers).

Please see previous response.

k. Exit Strategy –Define how this process would work and what costs would be involved. Is there a cost for transferred data?

If a customer ceases services, they have 90 days to retrieve their documents.

This transactional data may include:

Envelope addressing information

Sender account information

Envelope history

Specific envelope transaction information such as: IPs, date/time of signing/authentication methods, etc.

In addition, customers are free to purge those documents at any time and can use the API to verify that it has been completed. All aspects of each signed transaction are fully logged and captured in the detailed transaction history captured and stored as hashed, encrypted data associated with each sent and signed envelope. All events associated with a document processed on DocuSign are logged including send, sign, correct, reassign, deliver and view. The audit log of a document is kept permanently even if the underlying document is delivered and purged by the owning account. This maintains DocuSign's ability to prove a transaction indefinitely.

Using our Connect Service, there is no cost for transfer of data.

17. Service Level Agreement (SLA) and Reporting

The ideal solution will have a detailed Service Level Agreement (SLA)

a. Provide a copy of the proposed Service Level Agreement (SLA). Including notation of optional levels of service and Breaches in SLA from a Financial standpoint.

Please refer to the Copy of Vendor's License and Maintenance Agreements.

b. What is the standard service availability that the solution commits to provide in a Service Level Agreement (SLA)? Please provide quantitative response in percentage (%) and any other details to describe this service availability commitment.

Please refer to the Copy of Vendor's License and Maintenance Agreements.

c. Is the SLA Financially backed?

Please refer to Copy of Vendor's License and Maintenance Agreements.

d. With respect to RPO and RTO, please describe how the solution provided allows for an RPO of 24 hours and an RTO of 24-48 hours. Describe the architectural approach, infrastructure and operating environment that are necessary to meet the stated recovery point and time objectives. In addition, tell us if the proposed solution exceeds those metrics.

DocuSign's carrier-grade Architecture, a first in SaaS, features three simultaneously active & redundant systems that allow the overall system to service full site outages so it's "always on". Customer data is stored up to nine times across the three geographically disparate locations. RTO = 15 mins / RPO = 5 mins.

e. Describe report and metrics generation capabilities. Show examples of how utilization can be tracked by user or groups of users.

DocuSign standard dashboards and reporting would allow a sender to get perspective on historical and status related information of all envelopes/documents. The reporting tool also allows the sender to set schedules for the creation of these type of audit reports on a regular basis.

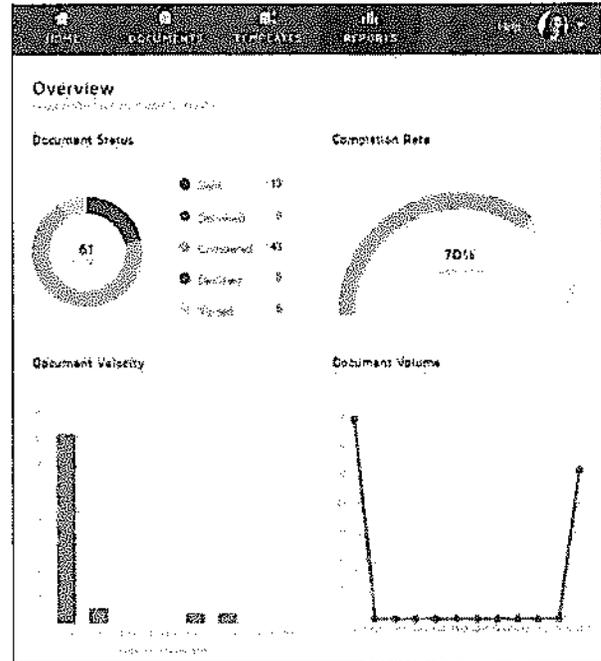
There are several pre-formatted Dashboard reports available in the console. These Dashboards provide drillable quick access to commonly requested envelope information. Each of the Dashboards is described below:

Overview: This option shows all the visual reports and reporting options.

In Process Envelopes: This option shows a list of envelopes that have been sent, but not signed, in the Results Panel, with a bar chart aging report showing the number of days since an envelope was sent for signature in the Detail Panel. Optionally, you can show the aging report for envelopes awaiting your signature.

Completed Envelopes: This option shows a list of envelopes that are completed in the Results Panel and a bar chart Time to Complete report showing the number of days between sending an envelope and completing the envelope in the Detail Panel.

Envelopes Status: This option shows a list of envelopes that have been sent in the Results Panel and a pie chart showing the status of the envelopes in the Detail Panel.



Standard Reports from the web console are divided into three categories - each being exportable and customizable:

DocuSign Standard Reports	
Envelope Reports	
Envelope Report	This report lists all envelopes for the selected report parameters. Each report row is for a different envelope and shows envelope status, the sender, the recipient(s) and activity information for the envelope.
Envelope Recipient Report	This report is similar to the Envelope Report but provides additional information about the recipients, their place in the routing order, how they were authenticated, and their actions.

SOLICITATION # ITS-400335

DocuSign Standard Reports	
Envelope Status Report	This report provides envelope totals sorted by status for the selected report parameters. Each report row is for a different envelope status and shows the total envelope with that status, the number of unique senders, the total recipients, the total signers, the total documents and total pages.
Envelope Velocity Report	This report provides information about envelope completion times for the selected report parameters.
Envelope Volume Report	This report provides information about envelopes sent, completed, corrected, declined and voided, along with the average completion time, for the selected report parameters.
Recipient Reports	
Recipient Activity Report	This report provides activity information for envelope recipients for the selected report parameters. Each report row is for a different recipient and shows the number of envelopes received, signed, not signed, a completion rate and the average time for that recipient to complete an envelope.
Recipient Authentication Report	This report provides information about the authentication methods used to verify the identity of users for the selected report parameters.
Usage Reports	
User Activity Report	This report provides activity information for account users for the selected report parameters. Each report row is for a different account user and shows the number of envelopes sent, completed, the number of templates created and the last envelope activity for each user.
Group Activity Report	This report provides activity information for groups in your account for the selected groups and timeframe. The report shows the number of users in each group, the number of envelopes sent, the number of envelopes completed, the number of templates created and the last envelope activity for a member of the group.
Account Activity Report	This report provides activity information for the account for the selected timeframe. The report shows the number of users in the account, the number of envelopes sent, the number of envelopes completed, the number of templates created and the last envelope activity for the account.

For more details: <https://10226ec94e53f4ca538f-0035e62ac0d194a46695a3b225d72cc8.ssl.cf2.rackcdn.com/quick-start-reporting.pdf>

f. The state will require a rolled-up view of all usage broken down by agency quarterly and yearly; therefore, describe how the solution will allow agencies to run their own usage reports.

DocuSign's reporting capabilities allow for the tracking of activities in the account. DocuSign's UI does not currently allow for reporting across multiple accounts. To have a rolled-up report of all activities across accounts from the state agencies, data will need to be extracted (and/or automatically pushed) into a data storage for more detailed reporting (ex: SQL). The use of a BI tool can handle the reporting needs across the entirety of the usage across all state agencies.

DocuSign Total Search – new feature

DocuSign's Total Search feature is described below and is not included in our pricing, since it is a new optional feature. We are happy to provide providing and additional information if requested.

DocuSign Total Search (powered by Seal) is designed to drive 'human discovery': it will enable customers to centralize all of their digital agreements, organize them using metadata (structural data), and search inside them using natural language terms (unstructured data). DocuSign Intelligent Insights (powered by Seal) is designed to drive 'machine discovery': it will use artificial intelligence and machine learning to automatically extract mission critical legal concepts like indemnification, warranty and most favored nation, among others. DocuSign Compliance Packs (powered by Seal) use the same artificial intelligence and machine learning to extract concepts derived from key regulations, including GDPR.

These integrated platform extensions from Seal, available later this year, bring powerful new capabilities to the 'manage' stage of modern Systems of Agreement. Customers can instantly and easily find agreements, regardless of their origin or storage location. They can then compare sections of similar agreements to identify inconsistent contracted terms, areas of exposure,

and potential revenue leakage. And they can review auto-extracted terms and concepts to ensure compliance and minimize exposure to risk.

g. The total transaction volume can be tracked by month, by Department/Division/Unit, and reported to DIT.

DocuSign provides a number of reports that include capabilities to see the activity based upon Recipients, Users, Groups, and overall Account activity. Additional filters are available and the reports can be scheduled to run automatically based on set criteria. These can be sent to Users and non-Users of DocuSign. The following reports can be used:

- Recipient Activity Report – This report provides activity information for envelope recipients for the selected report parameters. Each report row is for a different recipient and shows the number of envelopes received, signed, not signed, a completion rate and the average time for that recipient to complete an envelope.
- User Activity Report – This report provides activity information for account users for the selected report parameters. Each report row is for a different account user and shows the number of envelopes sent, completed, the number of templates created and the last envelope activity for each user.
- Group Activity Report – This report provides activity information for groups in your account for the selected groups and timeframe. The report shows the number of users in each group, the number of envelopes sent, the number of envelopes completed, the number of templates created and the last envelope activity for a member of the group.
- Account Activity Report – This report provides activity information for the account for the selected timeframe. The report shows the number of users in the account, the number of envelopes sent, the number of envelopes completed, the number of templates created and the last envelope activity for the account.

18. Software Support and Maintenance Services

The ideal solution will have established support and maintenance. Please explain the following regarding these services:

a. Describe how the service desk operates; i.e., service hours, escalation of problems, ticket tracking, reporting of metrics on availability, call scripts, repository of solutions, call back time etc.

Get the answers you need, the way you want them. DocuSign Customer Support is here to give you the assistance you need so that you get the results you expect. Our industry-leading, global support model is there to back you up, no matter where you do your business. We provide you access to the expertise you want, whether through our communities, our knowledge base and on-demand training, or our team of experienced technical support professionals, who know you and your solutions. And we are set up to work the way you want, whether by phone, chat, email or web.

SOLICITATION # ITS-400335

Deliverable	Enterprise Premier
24x7 System Availability Monitoring	✓
Self Service Resources, including DocuSign Community, Support Portal, Knowledge Base	✓
24x7 Sender and Signer Live Chat Support	✓
Online case Submission and Management	✓
Case Submission Response Time Target	2 hours
24x7 Live Phone Support	✓
Escalated Tier 2 Support	✓
DocuSign Demo/Sandbox Environment Access	✓
DocuSign Integration Support (APIs, Connectors)	✓
24x7 Global Emergency Support	✓
Emergency Response Time Target	30 minutes
Proactive Monitoring of Cases	✓
Adoption Network	✓
Administrator Certification Class	1 user
Technical Customer Success Manager*	✓

Support Services Explained

- **24x7 System Availability Monitoring:** DocuSign Trust Site for real-time system status and notifications
- **Support Portal and Knowledge Base:** Search for answers and submit Support requests
- **DocuSign Community:** Q&A community staffed by DocuSign employees and power users of our product
- **24x7 Sender and Signer Live Chat Support:** Chat Support for simple questions on signing, sending and account management
- **Online Case Submission and Management:** Submit cases online for assistance from our Support Team
- **24x7 Live Phone Support:** Talk to our DocuSign Support Team for technical DocuSign questions, billing inquiries and account support
- **Escalated Support - Tier 2:** Direct access to a senior technical resource as part of standard support escalation process.
- **DocuSign Demo/Sandbox Environment Access:** Test your current code against upcoming releases or add your new code to test prior to releasing into production
- **DocuSign Integration Support (Connectors):** Support for connections to complementary solutions such as Salesforce, Microsoft, and Google.
- **24x7 Emergency Support:** 30-minute response to Severity 1 technical incidents.

SOLICITATION # ITS-400335

- **Proactive Monitoring of Cases:** Ongoing tracking and review of cases opened to identify trends, possible issues, or opportunities for improved use of DocuSign
- **Deliverables:** CSA Certification course for one user through DocuSign University; 2-hours of office hour access to DocuSign CSA team; access to Adoption Network gated community
- **Technical Customer Support Manager:** First point of contact for all technical questions. Trained in customer use cases, workflows, and technology. Will provide case reviews on a regular basis as part of the relationship.

Please refer to the Copy of Vendor's License and Maintenance Agreements for additional details.

b. *Describe how the solution will provide availability and uptime metrics for solution.*

DocuSign provides a Trust Center to provide transparency into service performance, availability, and technical best practices. DocuSign's Trust Center is available here: <https://trust.docusign.com/>

While other vendors may claim a strong uptime, we invite the State to investigate our competitor's uptime records. Our closest competitor has frequently periods of downtime and large chunks of regularly scheduled maintenance. DocuSign is proud to report our historical uptime, which is the best in the industry.

- 2013 99.97% (does not include scheduled downtime)
- 2014 99.95% (last scheduled downtime was April 2014)
- 2015 99.9942%
- 2016 99.9954%
- 2017 99.9996% <https://trust.docusign.com/en-us/system-status/>

DocuSign provides a Trust Center to provide transparency into service performance, availability, and technical best practices. DocuSign's Trust Center is available here: <https://trust.docusign.com/>

A snap shot is provided below of the system status showing the last 12 months.

SYSTEM STATUS

ENVIRONMENT	Current Status	APP												MAR 19								
		5	4	3	2	1	31	30	29	28	27	26	25		24	23	22	21	20	19		
North America																						
NA1	100%																					
		2018					2017															
		Feb	Jan	Dec	Nov	Oct	Sep	Aug	Jul	Jun	May	Apr										
		100%	100%	100%	100%	100%	99.95%	100%	100%	100%	100%	100%										
NA2	100%																					
		2018					2017															
		Feb	Jan	Dec	Nov	Oct	Sep	Aug	Jul	Jun	May	Apr										
		100%	100%	100%	99.99%	100%	100%	100%	100%	99.99%	100%	100%										
NA3	100%																					
		2018					2017															
		Feb	Jan	Dec	Nov	Oct	Sep	Aug	Jul	Jun	May	Apr										
		100%	99.97%	100%	99.99%	99.99%	99.99%	100%	100%	99.99%	99.984%	100%										
DEMO	100%																					
		2018					2017															
		Feb	Jan	Dec	Nov	Oct	Sep	Aug	Jul	Jun	May	Apr										
		100%	100%	99.99%	100%	100%	100%	99.96%	100%	100%	100%											
Europe																						
EU	100%																					
		2018					2017															
		Feb	Jan	Dec	Nov	Oct	Sep	Aug	Jul	Jun	May	Apr										
		100%	100%	100%	100%	100%	100%	100%	99.91%	100%	100%	100%										
EU TSP	100%																					
Corporate																						
Headquarters	TBD																					
Customer Service	TBD																					
Learning Portal	100%																					

c. Describe the solution's development "sandbox" as envisioned for backend integration efforts with legacy environments.

The DocuSign Sandbox:

- Sandbox is a safe and secure test environment
- Test functionality, scalability, and performance before production release
- Early access to DocuSign innovations and code base
- Allows IT teams to maintain separate development and production environments

Benefits for the State

- Develop and test DocuSign custom integrations before production release
- Reduce business risk and development cycles by eliminating the need to develop in production
- Ensure business continuity by simulating different use cases and assessing real-world outcomes.

- Protect your DocuSign investment as test transactions don't impact production limits

QA Sandbox Overview

Enables IT teams to develop and test custom integrations

- Targeted to **medium and large** organizations who need to test DocuSign custom integrations
- Customers can perform **ongoing testing** at normal loads (up to 3x monthly average)
- Metadata retained for up to **30 days**
- Access to Engineering Services Engineer Consultants as an optional add-on

QA Sandbox Offering Details

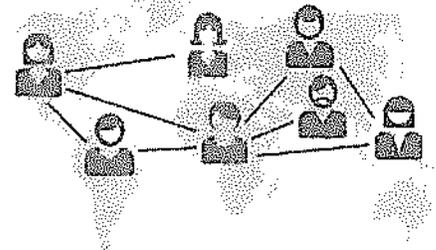
Simulated production environment	<ul style="list-style-type: none"> • Simulated production environment • Access to new features, bug fixes and updates at any time during business hours • Test transactions are not recorded and are not intended to be legally used
Metadata retention	<ul style="list-style-type: none"> • Metadata retained for 30 days with post-mortem support (up to 90 days) • Metadata includes customer email and IP address • Storage up to 100MB per 1000 test transactions per month per customer
Ongoing transaction testing	<ul style="list-style-type: none"> • Available to test normal loads at any time • 3x monthly average transaction volume through tests
Access to Engineering Services Engineer Consultants	<ul style="list-style-type: none"> • Available upon request for technical consulting • Access to optional call center support • Technical support is dependent on availability
Performance testing	<ul style="list-style-type: none"> • Not available

DocuSign

High-Performance Sandbox Overview

Gives enterprise IT teams the ability to test performance and custom integrations in highly scalable environments

- Designed for IT teams in large enterprises that need to regularly test performance, surge, and scalability
- Customers can perform ongoing testing at normal loads (up to 3x monthly average)
- Up to 1 performance/surge test period per quarter
- Metadata retained for up to 1 year
- Access to a dedicated Professional Services Senior Engineer



DocuSign is the only vendor that supports a high-performance Sandbox.

SOLICITATION # ITS-400335

d. Describe how the application changes will be able to be previewed in a "sandbox"/non-production environment prior to changes being made in production.

DocuSign conducts rolling product releases and patches to the system without any downtime to the agencies. All updates and enhancements are released to the Sandbox environment prior to Production release.

The DocuSign Sandbox is a safe and secure test environment that can be used to:

- Test functionality, scalability, and performance before production release
- Early access to DocuSign innovations and code base
- Allows IT teams to maintain separate development and production environments

e. Describe the management and project team assigned to work with North Carolina.

The DocuSign Account Management Team consists of an Account Executive, Solution Engineer, Account Manager, and likely a Customer Success Architect. The Account Executive and Solution Engineer focus heavily on sales and ensuring the customer understands where and how the DocuSign solution can provide value. Key responsibilities of the Account Manager include being a primary point of contact throughout the life cycle of the client relationship, ensuring overall success and satisfaction, providing customer service support and troubleshooting issues for assigned accounts.

The Customer Service Architect is a fee-based role who will champion DocuSign adoption within the customer enterprise by providing leadership and driving the identification and ROI justification of use cases for the DocuSign solution. The CSA will provide creative solutions to key obstacles preventing customer adoption. The CSA will be representing DocuSign to the most strategic customers and will ensure exceptional customer satisfaction.

Regarding additional resources which may be assigned to the State's team, DocuSign assigns resources (which are full-time DocuSign Staff) on a first come first serve basis from the date of mutual acceptance of the Statement of Work (SOW). From that date, we need one to two weeks to schedule those resources which need to be considered in your planning.

f. Describe the process for incident management, change management and release management.

DocuSign maintains an ISO 27001, PCI DSS, and SSAE16 examined and tested Incident Response Program and Breach Notification policies and processes. All incidents are to be reported via a standard internal form to ensure consistency of information capture.

Customer Contacts

DocuSign's Contracts Manager retains the list of customers requiring specific notification within specific timeframes. Upon detection of any customer information within DocuSign's control that may have been improperly accessed or acquired by an unauthorized party, DocuSign references the data accessed to determine the type of exposure, the population of customers impacted, and the nature of the acquiring individual or entity.

Prompt Notifications

DocuSign maintains a data breach notification program to promptly notify customers in the event their information is lost or experiences unauthorized access. DocuSign will promptly notify customers in the event that their protected data is reasonably believed to be lost or stolen in an unencrypted format, or subject to unauthorized access by, or is used or disclosed as a result of an unauthorized acquisition. DocuSign will provide notice in writing promptly after discovery of such a security incident, but in no event later than the deadline set forth under applicable Law or the applicable business agreement, whichever is earlier.

The written notice shall include, to the extent known, an identification of each individual whose personal information has been affected by the security incident, including state of residence; a brief description of the categories of personal information

SOLICITATION # ITS-400335

involved for each affected individual; a brief description of how and when the security incident occurred and how and when the security incident was discovered; and a brief description of any steps taken to address the security incident and any steps taken to prevent a recurrence.

To the extent this information is not known when the initial written notice is first provided, DocuSign will promptly supplement the written notice, in writing when information becomes known (unless specifically directed otherwise by a law enforcement organization).

Incident Management

DocuSign's formal Incident Response program aligns with the National Incident Management System - "D" Guidelines to contain, communicate, and resolve

- Initial Detection
- Initial Tactical Response
- Incident Briefing
- Refined Response
- Communication & Messaging
- Formal Containment
- Formal Incident Report
- Post Mortem/Trend Analysis

Change Management

DocuSign maintains ISO 27001, PCI DSS, SSAE18 and FedRAMP certifications. External auditors examined and tested Change Control policy and processes. All changes made to DocuSign Product Operations systems, Information, and devices are managed via the DocuSign tool. Changes are subjected to a testing regimen defined by IT and Technical Operations, which includes comprehensive scanning.

Technology systems, network devices, security devices, Active Directory objects or logging and alerting mechanisms must be authorized prior to the change being made in accordance with a specifically defined and documented approval process.

All changes are documented and approved via the DocuSign tool.

DocuSign performs extensive pre-deployment testing as the preferred method for assurance of changes promoted into the production environment.

Release Management

These are outlined in our Release Management policies which are ISO27001, PCI DSS, SSAE18, and FedRAMP examined and certified. DocuSign maintains policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities.

DocuSign has 4 releases each year. For more information, please see the DocuSign Release Notes page:
<https://support.docusign.com/en/releasenotes>

DocuSign implements a formal SDLC that is fully documented and audited as part of its SSAE 16 audit and ISO 270001 certifications. Code is developed in individual development environments through developer unit test and then deployed to a formal QA environment for testing, verification and requirements review by the separate QA and product management teams.

SOLICITATION # ITS-400335

g. Provide a list and description of the required roles and level of staff resources to manage, monitor, maintain and support the overall solution.

Title	Description
Support Escalation Manager	Customer support manager who will be an escalation path should the Customer L1/L2 Support be unable to resolve the issue.
Developers/Engineer	Developers/Engineers should make any adjustments and test solutions from end to end to ensure there are no disruption to services for each DocuSign release.
Release Manager	Release Managers are responsible for managing the DocuSign calendar and releases and develop a release plan. The release plan should include regression testing and a rollback strategy.
Customer L1/L2 Support	Customer L1/L2 Support are teams that end users should contact if there are issues after a release. Customer L1/L2 support should be fully trained on new feature releases, known issues, and steps for resolving issues.
DocuSign Administrators	DocuSign administrators should monitor the release schedule and participate in the release plan associated to confirming all use cases are functioning as expected.
Business Subject Matter Experts	Business SME's may be needed to validate use cases and processes are functioning as expected especially for larger releases with several features that impact existing solutions.

19. Training

The State desires a solution that will employ training techniques with the capability to accommodate various levels of users. Training will be needed for each department/division/unit to include form modification, workflow creation/modifications, and assistance with onboarding users including signature creation. Describe the solution's training regarding:

a. What modes of user training are available?

DocuSign offers training on-site or via WebEx.

Maximize your DocuSign rollout success with experienced instructors in a convenient virtual format. DocuSign University's End User Training allows your organization to leverage experienced instructors to support your successful roll-out through tailored virtual training. After DocuSign's Onboarding Success Consulting team onboard your Administrators, DSU's instructors develop and deliver customized virtual training sessions to prepare your company's DocuSign users with basic skills.

End User Training is ideal for large companies or departments looking to increase DocuSign adoption with a broad user group or complicated rollout.

- Basic DocuSign Skills
- Custom Integration Rollout
- DocuSign Mobile Tools
- Targeted Advanced Training
- Q&A "Office Hours"
- And Many More!

b. What level of training comes with the proposal?

Please see **Section 2 - Product Strategy Roadmap**, the 12-month Vendor Roadmap information, which includes free training developed specifically for the State.

c. *What type of training will be provided in the proposal for the new use cases and purchases? (to include form modification, workflow creation/modifications, and assistance with on-boarding users including signature creation.)*

Please see **Section 2 - Product Strategy Roadmap**, the 12-month Vendor Roadmap information, which includes free training developed specifically for the State and includes forms, workflow, and onboarding.

d. *What online help capabilities are available for users?*

DocuSign Customer Support gives you the ability to choose the right level of ongoing assistance you need to get the value you expect from our platform. Our industry-leading global support model is there to back you up, no matter where you are or how you want to engage – whether it's on the web, via online case management, live chat, phone or our team of dedicated technical support professionals on-hand 24x7, who know your solution inside and out.

DocuSign Support Center

The **DocuSign Support Center**, <https://support.docusign.com/>, is a free resource which provides a comprehensive library of reference documents and videos which take you step-by-step through the process. DocuSign's Support Center also includes a Case Management dashboard for logged in users.

Other Self-Service Support Resources

You'll also benefit from on-demand access to an extensive digital library of self-service resources including an active support community, an extensive knowledge base, product video tutorials and current release notes. At the end of the day, we strive to maintain a high standard of service and expert advice which results in a growing community of satisfied customers.

DocuSign Support Community, <https://support.docusign.com/forum>, – an online forum where you can access help, ask questions, and collaborate with other DocuSigners. Community Moderators review posts to make sure they are helpful and appropriate.

Knowledge Market, <https://support.docusign.com/en/knowledgemarket> – provides tools and tips on how to drive adoption of DocuSign. Some of the available resources are white papers, value studies, videos, and tools.

DocuSign University Learning Portal, <https://support.docusign.com/en/docusignuniversity> - a self-service learning tool utilized by customers throughout their DocuSign journey – beginning with your onboarding experience all the way to becoming a DocuSign expert. Users can browse self-paced learning paths and curated courses by role and type, as well as have access to DocuSign's entire training catalog.

e. *What online help capabilities are available for administrators?*

DocuSign Customer Support gives you the ability to choose the right level of ongoing assistance you need to get the value you expect from our platform. Our industry-leading global support model is there to back you up, no matter where you are or how you want to engage – whether it's on the web, via online case management, live chat, phone or our team of dedicated technical support professionals on-hand 24x7, who know your solution inside and out.

DocuSign Support Center

The **DocuSign Support Center**, <https://support.docusign.com/>, is a free resource which provides a comprehensive library of reference documents and videos which take you step-by-step through the process. DocuSign's Support Center also includes a Case Management dashboard for logged in users.

Other Self-Service Support Resources

You'll also benefit from on-demand access to an extensive digital library of self-service resources including an active support community, an extensive knowledge base, product video tutorials and current release notes. At the end of the day, we strive to maintain a high standard of service and expert advice which results in a growing community of satisfied customers.

DocuSign Support Community, <https://support.docusign.com/forum>, – an online forum where you can access help, ask questions, and collaborate with other DocuSigners. Community Moderators review posts to make sure they are helpful and appropriate.

Knowledge Market, <https://support.docusign.com/en/knowledgemarket> – provides tools and tips on how to drive adoption of DocuSign. Some of the available resources are white papers, value studies, videos, and tools.

DocuSign University Learning Portal, <https://support.docusign.com/en/docusignuniversity> - a self-service learning tool utilized by customers throughout their DocuSign journey – beginning with your onboarding experience all the way to becoming a DocuSign expert. Users can browse self-paced learning paths and curated courses by role and type, as well as have access to DocuSign's entire training catalog.

f. *What web-based documentation is provided?*

The **DocuSign Support Center**, <https://support.docusign.com/>, is a free resource which provides a comprehensive library of reference documents and videos which take you step-by-step through the process. DocuSign's Support Center also includes a Case Management dashboard for logged in users.

Other Self-Service Support Resources

You'll also benefit from on-demand access to an extensive digital library of self-service resources including an active support community, an extensive knowledge base, product video tutorials and current release notes. At the end of the day, we strive to maintain a high standard of service and expert advice which results in a growing community of satisfied customers.

DocuSign Support Community, <https://support.docusign.com/forum>, – an online forum where you can access help, ask questions, and collaborate with other DocuSigners. Community Moderators review posts to make sure they are helpful and appropriate.

Knowledge Market, <https://support.docusign.com/en/knowledgemarket> – provides tools and tips on how to drive adoption of DocuSign. Some of the available resources are white papers, value studies, videos, and tools.

DocuSign University Learning Portal, <https://support.docusign.com/en/docusignuniversity> - a self-service learning tool utilized by customers throughout their DocuSign journey – beginning with your onboarding experience all the way to becoming a DocuSign expert. Users can browse self-paced learning paths and curated courses by role and type, as well as have access to DocuSign's entire training catalog.

g. *What live and web-based technical support is provided?*

Depending on the support packaged purchased, the State will have access to the following live and web-based support options:

- **24x7 System Availability Monitoring:** DocuSign Trust Site for real-time system status and notifications
- **Support Portal and Knowledge Base:** Search for answers and submit Support requests
- **DocuSign Community:** Q&A community staffed by DocuSign employees and power users of our product

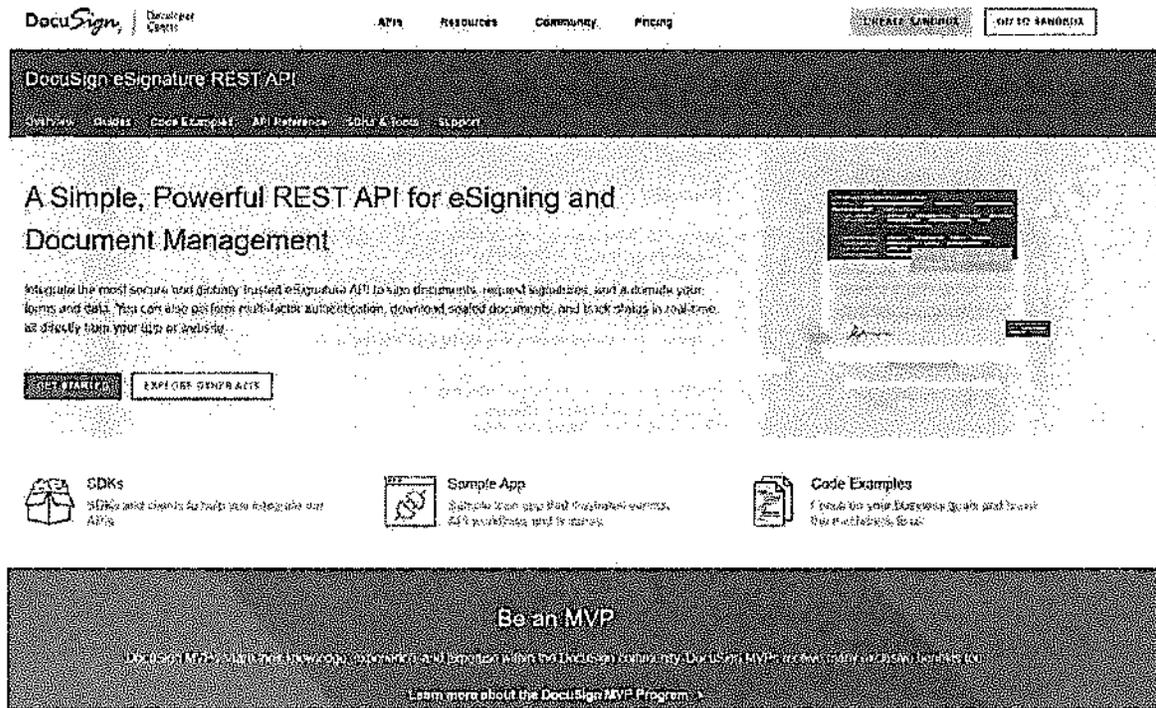
SOLICITATION # ITS-400335

- **24x7 Sender and Signer Live Chat Support:** Chat Support for simple questions on signing, sending and account management
- **Online Case Submission and Management:** Submit cases online for assistance from our Support Team
- **24x7 Live Phone Support:** Talk to our DocuSign Support Team for technical DocuSign questions, billing inquiries and account support
- **Escalated Support - Tier 2:** Direct access to a senior technical resource as part of standard support escalation process.
- **DocuSign Demo/Sandbox Environment Access:** Test your current code against upcoming releases or add your new code to test prior to releasing into production
- **DocuSign Integration Support (Connectors):** Support for connections to complementary solutions such as Salesforce, Microsoft, and Google.
- **24x7 Emergency Support:** 30-minute response to Severity 1 technical incidents.
- **Proactive Monitoring of Cases:** Ongoing tracking and review of cases opened to identify trends, possible issues, or opportunities for improved use of DocuSign
- **Deliverables:** CSA Certification course for one user through DocuSign University; 2-hours of office hour access to DocuSign CSA team; access to Adoption Network gated community
- **Technical Customer Support Manager:** First point of contact for all technical questions. Trained in customer use cases, workflows, and technology. Will provide case reviews on a regular basis as part of the relationship.

h. What types of training and documentation is provided for API usage?

The Developer Center, <https://developers.docusign.com/>, is the central portal for all resources and information that a developer needs to create apps and integrations for DocuSign products. It is geared toward beginner and experienced developers alike. The Developer Center contains all resources that developers need to get started, including:

- Quick-start guides
- API reference information
- API documentation for all API families
- Software Development Kits (SDKs) in all the popular development languages (C#, Java, Node.js, PHP, Objective-C, and more)
- Development tools
- Developer newsletter sign-up
- Additional resources (developer blog, MVP program, support info, etc.)



i. Describe the ability to provide cloud based user “sandbox” areas to support user on boarding, training, and functional trials. Specifically discuss limitations as related to function of the production system as well as trial or usage limits.

The DocuSign Sandbox:

- Sandbox is a safe and secure test environment
- Test functionality, scalability, and performance before production release
- Early access to DocuSign innovations and code base
- Allows IT teams to maintain separate development and production environments

Benefits for the State

- **Develop and test** DocuSign custom integrations before production release
- **Reduce business risk and development cycles** by eliminating the need to develop in production
- **Ensure business continuity** by simulating different use cases and assessing real-world outcomes
- **Protect your DocuSign investment** as test transactions don't impact production limits

QA Sandbox Overview

Enables IT teams to develop and test custom integrations

- Targeted to **medium and large** organizations who need to test DocuSign custom integrations
- Customers can perform **ongoing testing** at normal loads (up to 3x monthly average)
- Metadata retained for up to **30 days**
- Access to Engineering Services Engineer Consultants as an optional add-on

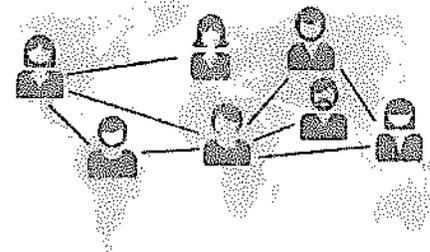
QA Sandbox Offering Details

Simulated production environment	<ul style="list-style-type: none"> • Same code as production (up to 3 weeks early for those code loads) • Access to environment (including full analytics) as any time during contract period • Test transactions are not marked and do not interfere with production
Metadata retention	<ul style="list-style-type: none"> • Retention: 30 days post last transaction (ETP) or end of 30 days • Includes transaction, envelope data, and responses • Storage up to 50MB per file (50MB per file) per file per user
Ongoing transaction testing	<ul style="list-style-type: none"> • Freedom to test normal loads at any time • To simulate a surge transaction from ongoing results through term
Access to Engineering Services Engineer Consultants	<ul style="list-style-type: none"> • Available as an option for extended consulting • Available for optimal coding/architecture • Technical support for diagnostic test results
Performance testing	<ul style="list-style-type: none"> • Not available

High-Performance Sandbox Overview

Gives enterprise IT teams the ability to test performance and custom integrations in highly scalable environments

- Designed for IT teams in large enterprises that need to regularly test performance, surge, and scalability
- Customers can perform ongoing testing at normal loads (up to 3x monthly average)
- Up to 1 performance/surge test period per quarter
- Metadata retained for up to 1 year
- Access to a dedicated Professional Services Senior Engineer



DocuSign is the only vendor that supports a high-performance Sandbox.

j. Describe whether the proposed solution requires customer to procure or implement any additional, on-premise hardware or technology commodities for proposed solution to function. Specify requirements by including descriptions, manufacturers, and model numbers.

DocuSign does not require the State to procure or implement any on-premise hardware or technology.

k. Provide information regarding user communities and/or support groups.

DocuSign Customer Support gives you the ability to choose the right level of ongoing assistance you need to get the value you expect from our platform. Our industry-leading global support model is there to back you up, no matter where you are or how you want to engage – whether it's on the web, via online case management, live chat, phone or our team of dedicated technical support professionals on-hand 24x7, who know your solution inside and out.

DocuSign Support Center

The **DocuSign Support Center, <https://support.docusign.com/>**, is a free resource which provides a comprehensive library of reference documents and videos which take you step-by-step through the process. DocuSign's Support Center also includes a Case Management dashboard for logged in users.

Other Self-Service Support Resources

You'll also benefit from on-demand access to an extensive digital library of self-service resources including an active support community, an extensive knowledge base, product video tutorials and current release notes. At the end of the day, we strive to maintain a high standard of service and expert advice which results in a growing community of satisfied customers.

DocuSign Support Community, <https://support.docusign.com/forum>, – an online forum where you can access help, ask questions, and collaborate with other DocuSigners. Community Moderators review posts to make sure they are helpful and appropriate.

Knowledge Market, <https://support.docusign.com/en/knowledgemarket> – provides tools and tips on how to drive adoption of DocuSign. Some of the available resources are white papers, value studies, videos, and tools.

SOLICITATION # ITS-400335

DocuSign University Learning Portal, <https://support.docusign.com/en/docusignuniversity> - a self-service learning tool utilized by customers throughout their DocuSign journey – beginning with your onboarding experience all the way to becoming a DocuSign expert. Users can browse self-paced learning paths and curated courses by role and type, as well as have access to DocuSign's entire training catalog.

D. COMPLETED COST OFFER

1) *Vendor shall be able to accept individual and/or Agency Wide Purchases on behalf of the agency and count toward the tiered pricing of that Agency.*

Yes. DocuSign can accept individual and/or Agency wide purchases which will count towards the tiered pricing of the Agency.

2) *Can Transactions/licensing fees be billed by Department/Division/Unit?*

Yes. DocuSign can bill directly to the department/division/unit.

3) *Pricing based on total transaction volume for the State.*

Yes. DocuSign's pricing is based on total volume purchased by Agency's leveraging the state contract.

4) *Explain usage and meaning of document, folder, and transaction system identifiers. Usage counts will need to correspond with Cost Proposal in Section IV.*

A transaction will be billed each time someone clicks "send" from or through a DocuSign production environment whether that is initiated through a connector, API, or web console. A transaction can have multiple documents, and/or "Signers" as long as it is one "send".

5) *Describe the purchase process for an Agency.*

DocuSign's proposed solution is structured to make the process easy for the Agency and DIT. The Agency can request a quote through DocuSign or Carahsoft and either DocuSign or Carahsoft will provide a quote based off the State contract. The contract will be finalized once the Agency cuts a PO and sends it to Carahsoft.

6) *Define the minimum transaction purchase.*

A minimum purchase of 1,000 Transactions is required.

7) *Define the Costs for Connectors to SharePoint, Dynamics 365, Salesforce etc.*

a. *What costs are there to integrate into SharePoint?, Azure, Amazon Webservices, Dynamics 365, and Salesforce.com.*

The connectors listed in our pricing table have a cost per user of \$144.00/year. Additionally, if you want us to stand up the connectors and do any development we charge professional services at a rate of \$295.00/hour. These include DocuSign Connector – Alfresco, DocuSign Connector - Google Enterprise Apps; DocuSign Connector - Microsoft Dynamics CRM, DocuSign Connector - Microsoft SharePoint, DocuSign Connector – NetSuite, DocuSign Connector – SugarCRM, DocuSign Connector – SAP, DocuSign Connector – Salesforce, DocuSign Connector – Ariba, and DocuSign Connector – SuccessFactors.

SOLICITATION # ITS-400335

b) *What other CRM solutions or cloud solutions do you integrate with? Provide list and a cost for each.*

Detailed pricing is included in our cost proposal below.

- Salesforce: The cost per user is \$144.00/year. The Salesforce Fast Start consulting package is priced at \$13,000.
- If the State wants DocuSign to stand up the connectors and perform development, we charge professional services at a rate of \$295.00/hour.
- Additional integrations: There are many other integrations available including SAP, Oracle, IBM, Google, Laserfiche etc. These connectors were developed by outside organizations and pricing can be obtained directly from those organizations.

8) *Define what is included in the Named users, Tiered, and unlimited pricing models. Support, training, adoption etc..*

Adoption Quick Start and Enterprise Premier Support is included in the pricing. Additionally, we offer more extensive implementation packages to stand up your instance. Please see the assorted "Fast Start Packages in the pricing matrix.

9) *Define Unlimited or Enterprise in terms of who can utilize this model.*

We do not offer unlimited models. We do offer transaction-based models which means you can licenses anyone within a participating agency and are only restricted by the number of sends they have available.

10) *Define what constitutes a transaction from a cost standpoint? Specifically, Voided Transactions and bulk Downloads.*

A transaction is counted every time you click "send". Voided transactions will count against your transaction allotments. Bulk downloads of documents are not considered transactions as they don't require you to hit the send button.

11) *Define Adoption accelerator costs if offered?*

Adoption Accelerator is not offered.

12) *Define the service level, description and costs for Standard, Premium, and Dedicated Support?*

DocuSign has detailed information in Question 18. Software Support and Maintenance Services. For ease of review, we also included it below.

Get the answers you need, the way you want them. DocuSign Customer Support is here to give you the assistance you need so that you get the results you expect. Our industry-leading, global support model is there to back you up, no matter where you do your business. We provide you access to the expertise you want, whether through our communities, our knowledge base and on-demand training, or our team of experienced technical support professionals, who know you and your solutions. And we are set up to work the way you want, whether by phone, chat, email or web.

Deliverable	Enterprise Premier
24x7 System Availability Monitoring	✓
Self Service Resources, including DocuSign Community, Support Portal, Knowledge Base	✓
24x7 Sender and Signer Live Chat Support	✓
Online case Submission and Management	✓
Case Submission Response Time Target	2 hours
24x7 Live Phone Support	✓
Escalated Tier 2 Support	✓
DocuSign Demo/Sandbox Environment Access	✓
DocuSign Integration Support (APIs, Connectors)	✓
24x7 Global Emergency Support	✓
Emergency Response Time Target	30 minutes
Proactive Monitoring of Cases	✓
Adoption Network	✓
Administrator Certification Class	1 user
Technical Customer Success Manager	✓

Support Services Explained

- **24x7 System Availability Monitoring:** DocuSign Trust Site for real-time system status and notifications
- **Support Portal and Knowledge Base:** Search for answers and submit Support requests
- **DocuSign Community:** Q&A community staffed by DocuSign employees and power users of our product
- **24x7 Sender and Signer Live Chat Support:** Chat Support for simple questions on signing, sending and account management
- **Online Case Submission and Management:** Submit cases online for assistance from our Support Team

SOLICITATION # ITS-400335

- **24x7 Live Phone Support:** Talk to our DocuSign Support Team for technical DocuSign questions, billing inquiries and account support
- **Escalated Support - Tier 2:** Direct access to a senior technical resource as part of standard support escalation process.
- **DocuSign Demo/Sandbox Environment Access:** Test your current code against upcoming releases or add your new code to test prior to releasing into production
- **DocuSign Integration Support (Connectors):** Support for connections to complementary solutions such as Salesforce, Microsoft, and Google.
- **24x7 Emergency Support:** 30-minute response to Severity 1 technical incidents
- **Proactive Monitoring of Cases:** Ongoing tracking and review of cases opened to identify trends, possible issues, or opportunities for improved use of DocuSign
- **Deliverables:** CSA Certification course for one user through DocuSign University; 2-hours of office hour access to DocuSign CSA team; access to Adoption Network gated community
- **Technical Customer Support Manager:** First point of contact for all technical questions. Trained in customer use cases, workflows, and technology. Will provide case reviews on a regular basis as part of the relationship.

13) *Is Unlimited phone technical support available for users, power users and administrators?*

Yes. DocuSign offers unlimited 24/7 support for all users, power users, administrators, and document recipients via Phone, Chat, or email.

Customer Support Operating Hours & Languages

General Customer Support

There are many ways (phone, chat, email or web communities and knowledge base) for customers and employees who are wishing to escalate customer issues to contact Customer Support depending on what service-level package the customer has purchased or the urgency of an issue.

Operating Hours

Support Levels	Free	Plus	Premier	Enterprise
Contact Method (Channel)	Online Case Chat Phone	Online Case Chat Phone Click-to-Call	Online Case Chat Phone Click-to-Call Email	Online Case Chat Phone Click-to-Call Email

SOLICITATION # ITS-400335

Support Levels	Free	Plus	Premier	Enterprise
Hours of availability.*	24/7 7 days a week	Sun: 2:30 – 11 PM PT Mon - Thurs: 24/7 Fri: 12 AM – 8 PM PT	Sun: 2:30 – 11 PM PT Mon - Thurs: 24/7 Fri: 12 AM – 8 PM PT	Sun: 2:30 – 11 PM PT Mon - Thurs: 24/7 Fri: 12 AM – 8 PM PT

DocuSign Support Center

The **DocuSign Support Center**, <https://support.docusign.com/>, is a free resource which provides a comprehensive library of reference documents and videos which take you step-by-step through the process. DocuSign's Support Center also includes a Case Management dashboard for logged in users.

14) *Define what happens to the number of Transactions that are not used during the contract term and yearly anniversary.*

Any transactions not used by the end of the contract period expire and do not roll over to the next subscription year.

15) *Define the licensing model offered and how signatures and transactions are counted.*

DocuSign is offering a transaction-based model which does not count signatures, only transactions. A transaction is counted every time you hit the send button from DocuSign web console, through an API, or from a connector. A transaction can have multiple signers and multiple documents if it is triggered at the same time and goes to the same people.

16) *NCID Integration-This is a de-centralized model and each Agency will have its own solution; therefore, define the cost for integration. Consider*

a) *Storage – How much storage is included with each cost model.*

DocuSign offers unlimited storage of all documents routed with DocuSign.

b) *Exit Strategy – Define the cost for downloading transactions-Define how this process works*

With DocuSign, there is no cost for downloading transactions. There are several options for downloading transactions.

- Download them manually
- Use an API call to pull your documents to another location
- Or you can manually pull them down

SOLICITATION # ITS-400335

c) *What is the cost for bulk retrieval of documents?*

If you use the API you would just need to develop the API listener and appropriate API call to pull the documents. Alternatively, if you use retrieve you would need to purchase the Retrieve Tool.

d) *Migration costs from existing signature systems*

Migration services can be completed using our consulting services at a cost of \$295.00/hour.

e) *Are there costs for Voided Transaction if any?*

A voided transaction is still considered a transaction, so your cost would be the same as your other transaction costs.

f) *Is there customization required or proposed addressing specification. If so, what is the cost.*

Since this is for a Master Contract, DocuSign would need to evaluate each individual use case proposed by individual agencies to determine if there was a need for customization or professional services. Once the request is submitted, we will scope the request and provide a Statement of Work (SOW).

g) *Are there additional modules required or proposed addressing specifications.*

Since this is for a Master Contract, DocuSign would need to evaluate each individual use case proposed by individual agencies to determine if additional modules are required.

h) *Are there any installation/conversion/integration/transition costs?*

As most of your system is currently on DocuSign there should be no conversion or Transition costs. As DocuSign is a cloud solution there should be no installation costs. Integration costs vary based on complexity and can be scoped out on a per instance basis at a rate of \$295.00/hour.

i) *Provide all training costs by type; user, admin, power user. What is included in each cost model.*

DocuSign has included free training for the State which includes on-demand and self-service training, free of charge. Some of the training courses offered are also live instructor led courses. Detailed information on this and additional training offerings are available in our **Product Strategy Roadmap** response. Customized training is also available and would need to be scoped and pricing is available after more detail is provided.

j) *Maintenance costs per year- Is this an evergreen product and updates are included?*

A. DocuSign is a SaaS product and is therefore an evergreen product and updates are included.

SOLICITATION # ITS-400335

k) Do you have a professional consulting service or other value-added service based on hourly rates? Provide your hourly costs. Travel and lodging expenses, if any, must be thoroughly described, and are limited by the State's Terms and Conditions.

295.00/per hour [Customer will be invoiced all costs associated with out-of-pocket expenses (including, without limitation, costs and expenses associated with meals, lodging, transportation and any other applicable business expenses) listed on the invoice as a separate line item. Reimbursement for out-of-pocket expenses in connection with performance of this SOW, when authorized, shall be in accordance with Customer's then-current published policies governing travel and associated business expenses, which information shall be provided by the Customer Project Manager.]

DocuSign's Pricing Response

Item #	QTY	Unit	Description	Ext. Cost
1.	1	User/year	Named User	
2.	5	Users/year	Named User	
3.	25	Users/year	Named User	
4.	100	Transaction/year	Package of signatures	
5.	500	Transaction/year	Package of signatures	
6.	2500	Transaction/year	Package of signatures	
7.	5000	Transaction/year	Package of signatures	
8.	10000	Transaction/year	Package of signatures	
9.	20000	Transaction/year	Package of signatures	
10.	50000	Transaction/year	Package of signatures	
11.	75000	Transaction/year	Package of signatures	
12.	100000	Transaction/year	Package of signatures	
13.	Unlimited	Transaction/year	Package of signatures	
14.	NA	NA	NCID integration	
15.	Storage	MB	Cost for Form Storage	
16.		Per Connector	Connector to Dynamics 365	
17.		Per Connector	Connector to Salesforce	
18.		Per Connector	Connector to SharePoint Online	
19.		Per Connector	Connector to SharePoint On Prem	
20.			Bulk retrieval of Transactions	
21.		Per hour?	Migration Costs	
22.	Vendor Define	Transaction/year	Costs for Voided Transactions	
23.	Vendor Define	Per hour	Professional Services	

carahsoft

DocuSign

SOLICITATION # ITS-400335

License/ Service	ListPrice	Unit of Measure
<i>DocuSign Business Pro Edition - Envelope Subscription</i>	\$ 2.01	Per Envelope for Quantities of 50,000 - 99,999
<i>DocuSign Business Pro Edition - Envelope Subscription</i>	\$ 1.97	Per Envelope for Quantities of 100,000 - 499,999
<i>DocuSign Business Pro Edition - Envelope Subscription</i>	\$ 1.94	Per Envelope for Quantities of 500,000 - 999,999
<i>DocuSign Business Pro Edition - Envelope Subscription</i>	\$ 1.91	Per Envelope for Quantities of 1,000,000+
<i>DocuSign Business Pro for Gov - Env</i>	\$ 2.22	Per Envelope for Quantities of 50,000 - 99,999
<i>DocuSign Business Pro for Gov - Env</i>	\$ 2.18	Per Envelope for Quantities of 100,000 - 499,999
<i>DocuSign Business Pro for Gov - Env</i>	\$ 2.15	Per Envelope for Quantities of 500,000 - 999,999
<i>DocuSign Business Pro for Gov - Env</i>	\$ 2.12	Per Envelope for Quantities of 1,000,000+
<i>DocuSign Business Pro with FedRAMP - Env</i>	\$ 3.05	Per Envelope for Quantities of 50,000 - 99,999
<i>DocuSign Business Pro with FedRAMP - Env</i>	\$ 3.01	Per Envelope for Quantities of 100,000 - 499,999
<i>DocuSign Business Pro with FedRAMP - Env</i>	\$ 2.98	Per Envelope for Quantities of 500,000 - 999,999
<i>DocuSign Business Pro with FedRAMP - Env</i>	\$ 2.95	Per Envelope for Quantities of 1,000,000+
<i>DocuSign Enterprise Pro Edition - Envelope Subs.</i>	\$ 4.62	Per Envelope for Quantities of 50,000 - 99,999
<i>DocuSign Enterprise Pro Edition - Envelope Subs.</i>	\$ 4.59	Per Envelope for Quantities of 100,000 - 499,999
<i>DocuSign Enterprise Pro Edition - Envelope Subs.</i>	\$ 4.56	Per Envelope for Quantities of 500,000 - 999,999

SOLICITATION # ITS-400335

<u>License/ Service</u>	<u>ListPrice</u>	<u>Unit of Measure</u>
<i>DocuSign Enterprise Pro Edition - Envelope Subs.</i>	\$ 4.52	Per Envelope for Quantities of 1,000,000+
<i>DocuSign Enterprise Pro for Gov - Env</i>	\$ 5.41	Per Envelope for Quantities of 50,000 - 99,999
<i>DocuSign Enterprise Pro for Gov - Env</i>	\$ 5.38	Per Envelope for Quantities of 100,000 - 499,999
<i>DocuSign Enterprise Pro for Gov - Env</i>	\$ 5.34	Per Envelope for Quantities of 500,000 - 999,999
<i>DocuSign Enterprise Pro for Gov - Env</i>	\$ 5.31	Per Envelope for Quantities of 1,000,000+
<i>DocuSign Enterprise Pro with FedRAMP - Env</i>	\$ 6.72	Per Envelope for Quantities of 50,000 - 99,999
<i>DocuSign Enterprise Pro with FedRAMP - Env</i>	\$ 6.69	Per Envelope for Quantities of 100,000 - 499,999
<i>DocuSign Enterprise Pro with FedRAMP - Env</i>	\$ 6.66	Per Envelope for Quantities of 500,000 - 999,999
<i>DocuSign Enterprise Pro with FedRAMP - Env</i>	\$ 6.63	Per Envelope for Quantities of 1,000,000+
<i>DocuSign Business Pro for Gov with Lightning Sales Cloud Professional Edition (Includes Enterprise & Premier+ Support)</i>	\$ 1,513.88	Per Seat Annual
<i>DocuSign Business Pro for Gov with Lightning Sales Cloud Enterprise Edition (Includes Premier+ Support)</i>	\$ 2,642.50	Per Seat Annual
<i>DocuSign Business Pro for Gov with Lightning Sales Cloud Unlimited Edition (Includes Premier+ Support)</i>	\$ 4,899.76	Per Seat Annual
<i>DocuSign Business Pro for Gov with Lightning Service Cloud Professional Edition (Includes Premier+ Support)</i>	\$ 1,515.88	Per Seat Annual
<i>DocuSign Business Pro for Gov with Lightning Service Cloud Enterprise Edition (Includes Premier+ Support)</i>	\$ 2,642.50	Per Seat Annual
<i>DocuSign Business Pro for Gov with Lightning Service Cloud Unlimited Edition (Includes Premier+ Support)</i>	\$ 4,899.76	Per Seat Annual
<i>DocuSign Business Pro for Gov with Lightning Force 100 (Includes Premier+ Support)</i>	\$ 1,513.88	Per Seat Annual

carahsoft



SOLICITATION # ITS-400335

<u>License/ Service</u>	<u>ListPrice</u>	<u>Unit of Measure</u>
<i>DocuSign Enterprise Pro for Gov with Lightning Sales Cloud Professional Edition (Includes Enterprise & Premier+ Support)</i>	\$ 1,128.62	Per Seat Annual
<i>DocuSign Enterprise Pro for Gov with Lightning Sales Cloud Enterprise Edition (Includes Premier+ Support)</i>	\$ 2,899.35	Per Seat Annual
<i>DocuSign Enterprise Pro for Gov with Lightning Sales Cloud Unlimited Edition (Includes Premier+ Support)</i>	\$ 5,156.61	Per Seat Annual
<i>DocuSign Enterprise Pro for Gov with Lightning Service Cloud Professional Edition (Includes Premier+ Support)</i>	\$ 1,770.73	Per Seat Annual
<i>DocuSign Enterprise Pro for Gov with Lightning Service Cloud Enterprise Edition (Includes Premier+ Support)</i>	\$ 2,899.35	Per Seat Annual
<i>DocuSign Enterprise Pro for Gov with Lightning Service Cloud Unlimited Edition (Includes Premier+ Support)</i>	\$ 5,156.61	Per Seat Annual
<i>DocuSign Enterprise Pro for Gov with Lightning Force 100 (Includes Premier+ Support)</i>	\$ 1,770.73	Per Seat Annual
<i>Enterprise Premier Support</i>	\$ 0.22	% of Recurring Fees
<i>Access Management w/SSO - Per Envelope</i>	\$ 1.26	Per Envelope
<i>Advanced Workflows Addon - Envelope Subs.</i>	\$ 2.52	Per Envelope
<i>E-Notary</i>	\$ 2.52	Per Envelope
<i>Template Creation Package - Per Template</i>	\$ 157.50	Per Template
<i>Consulting - Per hour</i>	\$ 309.75	Per Hour
<i>Customer Success Architect - Full time</i>	\$ 33,600.00	Per Month
<i>Customer Success Architect - Half time</i>	\$ 18,900.00	Per Month
<i>Customer Success Architect - Quarter time</i>	\$ 10,500.00	Per Month

SOLICITATION # ITS-400335

License/ Service	ListPrice	Unit of Measure
<i>DocuSign Connector - Alfresco</i>	\$ 151.20	Per Seat Annual
<i>DocuSign Connector - Google Enterprise Apps</i>	\$ 151.20	Per Seat Annual
<i>DocuSign Connector - Microsoft Dynamics CRM</i>	\$ 151.20	Per Seat Annual
<i>DocuSign Connector - Microsoft SharePoint</i>	\$ 151.20	Per Seat Annual
<i>DocuSign Connector - NetSuite</i>	\$ 151.20	Per Seat Annual
<i>DocuSign Connector - SugarCRM</i>	\$ 151.20	Per Seat Annual
<i>DocuSign Connector - SAP</i>	\$ 151.20	Per Seat Annual
<i>DocuSign Connector - Salesforce</i>	\$ 151.20	Per Seat Annual
<i>DocuSign Connector - Ariba</i>	\$ 151.20	Per Seat Annual
<i>DocuSign Connector - SuccessFactors</i>	\$ 151.20	Per Seat Annual
<i>API Certification</i>	\$ 1,050.00	Per Integration
<i>Fast Start API</i>	\$ 18,375.00	Flat Fee
<i>Authentication - Phone - Usage Subscription</i>	\$ 0.79	Per Envelope
<i>Authentication - SMS - Usage Subscription</i>	\$ 0.21	Per Envelope
<i>DSU DocuSign for Administrators Certification Course - Per Person</i>	\$ 1,785.00	Per Person
<i>Fast Start Salesforce.com</i>	\$ 13,650.00	Flat Fee

carahsoft

DocuSign

SOLICITATION # ITS-400335

<u>License/ Service</u>	<u>ListPrice</u>	<u>Unit of Measure</u>
Fast Start Web Console	\$ 9,975.00	Flat Fee
Fax Services - Envelope Subscription	\$ 0.11	Per Fax Page
Fax Services - Per Use	\$ 0.11	Per Fax Page
Full Service API	\$ 47,250.00	Flat Fee
Single Sign On	\$ 2,625.00	ProServ; Flat Fee
Web Console Template Set-up	\$ 309.75	Per Person
Adv. Administration (w/SSO) - for Seats Add-on (\$/seat)	\$ 126.00	Per Seat Annual
Training -	\$ -	
Authentication - Knowledge-Based (ID Check) - Usage Subscription	\$ 2.63	Per Envelope
Onboarding - Per Package	\$ 525.00	
Onboarding - Per Hour	\$ 262.50	
Momentum - San Francisco	\$ 1,044.75	Per Person
Training - Retrieve	\$ 309.75	Per Person
Training - Salesforce Admin	\$ 309.75	Per Person
Training - Web Console Admin	\$ 309.75	Per Person

DocuSign | The Global Standard for
Digital Transaction Management®

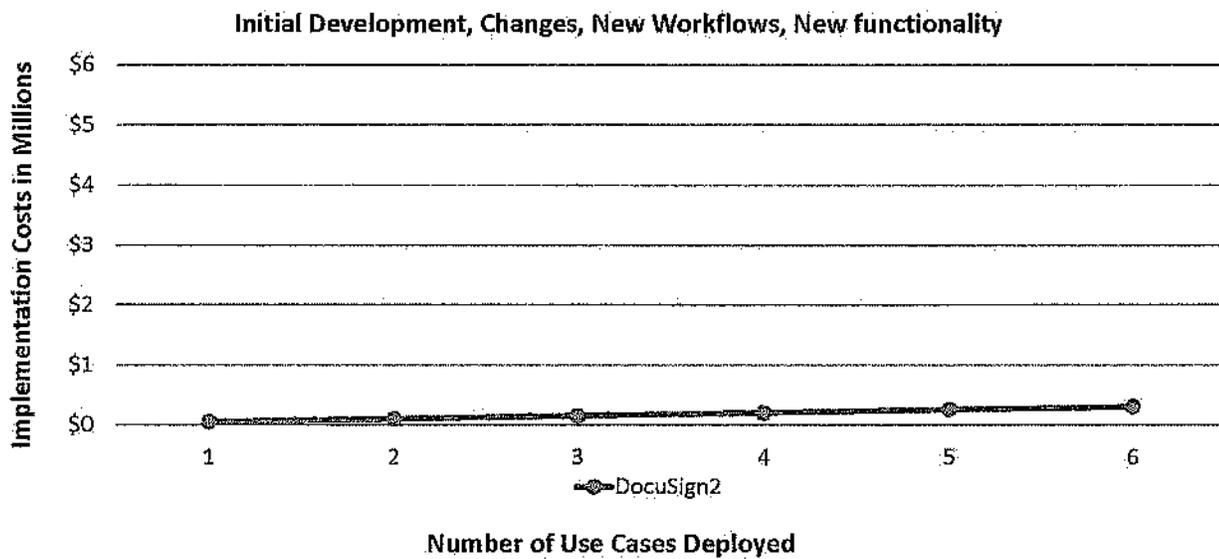
Total Cost of Ownership
North Carolina
July 2018

DocuSign Total Cost of Ownership – 1 Year

		DocuSign	
		One-Time	Annual Cost
Data Center Infrastructure	Hardware and Software (Document Server, Installation / Configuration)	included	included
	HW and SW Maintenance	included	included
Data Center Maintenance	Data Center Operations + IT support personnel	included	included
	Personnel and IT cost for managing on premise security of infrastructure	included	included
Services & Training	Total cost per use case deployments (set-up, customizations, integrations)	Not included	-
	Cost of lost benefits due to lower adoption of on premise solutions (based on Forrester research)	n/a	n/a
Product & Support	Product and Support (95,000 transactions)	\$181,355	
Grand Total		\$181,355	

Source: DocuSign Analysis based on Forrester Research Methodology

Solution Costs per Number of Use Cases deployed



Facts

- ✓ DocuSign is more expensive upfront with a lower TCO.
- ✓ DocuSign provides an ROI
- ✓ DocuSign is faster to deploy
- ✓ Greater adoption rate with SaaS
- ✓ Time is money
- ✓ Expansion into Enterprise wide
- ✓ Comparing DocuSign to our competitors is not apples to apples

Assumptions

- ✓ Overall ROI Numbers
- ✓ Competitors are Free

DocuSign, Inc. 2019

DocuSign



“Free” isn’t free.

E. REFERENCES**Reference #1**

Agency	NC DHHS
Name	Brenda K Williams
Title	Moodle E-Learning Coordinator
Email	brenda.williamson@dhhs.nc.gov
Scope of the Project	Internal Processes. E.g. Travel Requests

Reference #2

Agency	NC DOT
Name	Bryan Edwards
Title	Manager, CADD Services
Email	Bledwards1@ncdot.gov
Scope of the Project	Plan Documents (CAD Diagrams), HR Forms, and other internal forms.

Reference #3

Agency	NC Office of Comptroller
Name	Taylor Brumbeloe
Title	Central Compliance Manager
Email	Taylor.brumbeloe@osc.nc.gov
Scope of the Project	Merchant Authorization Forms

F. FINANCIAL INFORMATION

The Vendor shall provide evidence of financial stability with its response to this RFP as further described hereinbelow. As used herein, Financial Statements shall exclude tax returns and compiled statements.

- a) For a publicly traded company, Financial Statements for the past three (3) fiscal years, including at a minimum, income statements, balance sheets, and statement of changes in financial position or cash flows. If three (3) years of financial statements are not available, this information shall be provided to the fullest extent possible, but not less than one year. If less than 3 years, the Vendor must explain the reason why they are not available.*
- b) For a privately held company, when certified audited financial statements are not prepared: a written statement from the company's certified public accountant stating the financial condition, debt-to-asset ratio for the past three (3) years and any pending actions that may affect the company's financial condition.*
- c) The State may, in its sole discretion, accept evidence of financial stability other than Financial Statements for the purpose of evaluating Vendors' responses to this RFP. The State reserves the right to determine whether the substitute information meets the requirements for Financial Information sufficiently to allow the State to evaluate the sufficiency of financial resources and the ability of the business to sustain performance of this RFP award. Scope Statements issued may require the submission of Financial Statements and specify the number of years to be provided, the information to be provided, and the most recent date required.*

As a privately owned company, Carahsoft does not publicly release financial information. We are a stable, conservative, and profitable company which has grown, since founding in 2004, from \$4M in bookings to more than \$4.4B in 2017. The company has received numerous accolades for our business performance from our manufacturing partners and the industry, including annual recognition (detailed further on our website) in the CRN Solution Provider 500 (2006-2018), Washington Technology's Top 100 Government Contractors (2010-2017), and the Washington Business Journal's Largest Government Contractors (2011-2018).

We currently maintain a \$25M line of credit available (currently 100% available) with Union Bank.

Should you require our audited financial statements or have further financial inquiries, we would be happy to provide additional information under separate cover to the specific individual that would be reviewing them.

Specific questions may be referred to Craig P. Abod, President of Carahsoft Technology Corp.

G. CONFLICT OF INTEREST

i) Provide a statement that no assistance in preparing the response was received from any current or former employee of the State of North Carolina whose duties relate(d) to this RFP, unless such assistance was provided by the state employee in his or her official public capacity and that neither such employee nor any member of his or her immediate family has any financial interest in the outcome of this RFP;

Carahsoft Technology Corporation confirms that no assistance in preparing the response was received from any current or former employee of the State of North Carolina whose duties relate(d) to this RFP.

ii) State if the Vendor or any employee of the Vendor is related by blood or marriage to an Agency employee or resides with an Agency employee. If there are such relationships, list the names and relationships of said parties. Include the position and responsibilities within the Vendor's organization of such Vendor employees; and

None

iii) State the employing State Agency, individual's title at that State Agency, and termination date.

N/A

H. ERRATA AND EXCEPTIONS

Errata and Exceptions, if any. Offers conditioned upon acceptance of Vendor Exceptions may be determined to be non-responsive by the State.

N/A

I. COPY OF VENDOR'S LICENSE AND MAINTENANCE AGREEMENTS

Copy of the Vendor's License and Maintenance Agreements, if any. The State reserves the right to edit or modify these agreements to conform to the best interest of the State.

Please find the relevant Agreements beginning on the following page.

STATE OF NORTH CAROLINA Office of Information Technology Services STATEWIDE IT PROCUREMENT	REQUEST FOR BEST AND FINAL OFFER (BAFO) # 2 ITS-006375	
	Offers will be received until: August 10, 2012	
	Contract Type: Open Market	
Refer <u>ALL</u> Inquiries to: Tim Lassiter Telephone No. (919) 754-6526	Issue Date: August 8, 2012 Commodity: 920 – Enterprise-Wide Electronic Forms and Digital Signature	
E-Mail: tim.lassiter@nc.gov	Using Agency Name: Office of the State Controller	
(See page 2 for mailing instructions.)	Agency Requisition No. N/A	
http://www.its.state.nc.us/		

NOTICE TO VENDOR Offers, subject to the conditions made a part hereof, will be received at this office, 3900 Wake Forest Road, Raleigh, NC 27609, until 2:00 p.m. Eastern Standard Time on the day of opening and then opened, for furnishing and delivering the goods and services as described herein. Refer to page 2 for proper mailing instructions.

Bids submitted via facsimile (fax) machine in response to this Best and Final Offer (BAFO) will not be accepted. Bids are subject to rejection unless submitted on this form.

EXECUTION

In compliance with this Request for Best and Final Offers (BAFO), and subject to all the conditions herein, the undersigned offers and agrees to furnish and deliver any or all goods and services which are offered, at the prices agreed upon and within the time specified herein. Pursuant to GS § 147-33.100 and under penalty of perjury, the undersigned Vendor certifies that this offer has not been arrived at collusively or otherwise in violation of Federal or North Carolina law and this offer is made without prior understanding, agreement, or connection with any firm, corporation, or person submitting an offer for the same commodity, and is in all respects fair and without collusion or fraud.

Failure to execute/sign bid prior to submittal shall render bid invalid. Late bids are not acceptable.

BIDDER: DocuSign, Inc.		
STREET ADDRESS: 111 Sutter Street		P.O. BOX:
CITY & STATE & ZIP: San Francisco, CA, Suite 1000 94104		ZIP: 94104
TELEPHONE NUMBER: 415-489-4939		TOLL-FREE TEL. NO:
PRINT NAME & TITLE OF PERSON SIGNING: Joe Fuca Sr. Vice President, world wide sales		FAX NUMBER:
AUTHORIZED SIGNATURE: <i>Joe Fuca</i>	DATE: 8/8/2012	E-MAIL: joe.fuca@docusign.com

Offer valid for 60 days from date of bid opening unless otherwise stated here: _____ days

DS
CE

DS
LHD

ACCEPTANCE OF BEST AND FINAL OFFER

If the State accepts any or all parts of this offer, an authorized representative of Office of State Controller shall affix her/his signature to the Vendor's response to this Request for BAFO. The acceptance shall include the response to this BAFO, any provisions and requirements of the original RFP which have not been superseded by this BAFO, the first BAFO, the Vendor's response to the RFP. These documents shall then constitute the written agreement between the parties. A copy of this acceptance will be forwarded to the successful Vendor(s).

FOR OSC USE ONLY

Offer accepted and contract awarded this ___ day of _____, 20___, as indicated on attached certification,

by _____ (Authorized representative of the Office of the State Controller).

DELIVERY INSTRUCTIONS: Vendor must deliver one (1) **signed original** and two (2) **copies** of the Proposal to Issuing Agency in a sealed package with Company Name and RFP Number clearly marked on the front. Vendor must also submit one (1) signed, executed electronic copy of its proposal on read-only CD/DVD(s) or USB Drive. The files on the discs should not be password-protected and should be capable of being copied to other media.

Address envelope and insert bid number as shown below. Please note that the US Postal Service does not deliver any mail (US Postal Express, Certified, Priority, Overnight, etc.) on a set delivery schedule to this Office. **It is the responsibility of the Vendor to have the bid in this Office by the specified time and date of opening.**

DELIVER TO:

BID NUMBER: ITS-006375

Statewide IT Procurement Office

Attn: Tim Lassiter, Assistant Chief

3900 Wake Forest Road, Raleigh, NC 27609

Sealed bids, subject to the conditions made a part hereof, will be received at 333 E. Six Forks Road, 2nd floor Raleigh, NC, until 2:00 pm Eastern Standard Time on the day of opening and then opened, for furnishing and delivering the commodity as described herein. Proposals for this RFP must be submitted in a sealed package with the Execution of Proposal signed and dated by an official authorized to bind the Vendor's firm. Failure to return a signed execution of proposal shall result in disqualification. All proposals must comply with Section VI, Proposal Content and Organization.

Proposals **will not** be accepted by electronic means. This RFP is available electronically at <http://www.ips.state.nc.us/ips/pubmain.asp>. All inquiries regarding the RFP requirements are to be addressed to the contact person listed on Page One.

DIGITAL IMAGING: The State will digitize the Vendor's response if not received electronically, and any awarded contract together with associated contract documents. This electronic copy shall be a preservation record, and serve as the official record of this solicitation with the same force and effect as the original written documents comprising such record. Any printout or other output readable by sight shown to reflect such record accurately is an "original."

SOLICITATION REQUEST FOR BEST AND FINAL OFFER (BAFO):

This request is to acquire a best and final offer from vendor for best pricing and additional information. Your offer should integrate the previous response to the RFP and any changes listed below. Any individual vendor can receive a different number of requests for BAFOs than other bidders.

This Request for a Best and Final Offer, if accepted by the State, shall supersede all conflicting terms, and where terms or provisions of subordinate documents are modified herein, such terms shall fully replace the original terms of the subordinate documents.

Please Note: This bid is still in the evaluation period. During this period and prior to award, possession of the BAFO, original bid response and accompanying information is limited to personnel of the Statewide IT Procurement Office, and to agencies responsible for participating in the evaluation. Bidders who attempt to gain this privileged information, or to influence the evaluation process (i.e. assist in evaluation) will be in violation of purchasing rules and their offer will not be further evaluated or considered.

Table of Contents

Contents

Section VI. Other Specifications and Special Terms	9
Section VIII. North Carolina Information Technology Procurement Office General Terms and Conditions for Goods and Related Services	15

Special Terms of this Best and Final Offer:

1. The State selects an Envelope Allowance Subscription. The Office of the State Controller ("OSC") will purchase the Envelope Allowance Subscription, provisioning and Premier Support together with an Envelope Allowance of 100,000 Envelopes in each of the twelve (12) month periods comprising the initial two (2) year term. Payment for Platform Access will be made in two installments of \$355,000 corresponding with the two (2), twelve (12) month periods. OSC will issue one Purchase Order for the Envelope Allowance Subscription covering 24 months; other Purchase Orders may be used for recurring costs. The total Envelope Allowance purchase by OSC in the first Purchase Order, comprising 200,000 Envelopes, may be used at any time during the initial two (2) year term.
2. OSC's initial Purchase Order includes:
 - a. 24 month commitment for an Envelope Allowance subscription with an Envelope Allowance of 100,000 Envelopes/annually in each of the twelve (12) month periods comprising the initial twenty-four (24) month term,
 - b. Payment for this Envelope Allowance Subscription will be made in two installments of \$355,000 each,
 - c. Two Fast Start Implementation Integration Packages at \$15,000 each,
 - d. One Connect Express ("Fetch") license at \$15,000 (to be renewed annually at OSC's option),
 - e. 40 hours of Professional Services at \$7,800 to be available during the initial 24 month term, and
 - f. Options offered in the Vendor's RFP response, or other responsive documents, will be retained for exercise in the future.
3. Agencies may purchase Seat Subscriptions or Envelope Allowance Subscriptions at any time during the 24 month period for the balance of the 24 month initial term. In the event that an Agency's use of a Seat Subscription is determined to be abusive or unduly burdensome in accordance with the Software License (RFP Sec. VIII, 6) Software, as amended and incorporated herein, said Seat Subscription may be converted to an Envelope Allowance Subscription by mutual agreement of the Parties. For the avoidance of doubt, Table 1 illustrates Envelope Allowance Subscription purchasing and pricing, and Table 2 illustrates Seat Subscription purchasing and pricing.
 - a. Minimum purchase for an Envelope Allowance Subscription is 10,000 Envelopes.
 - b. Agencies may aggregate purchases to meet the minimum this Envelope Allowance purchase requirement. Agency purchasing aggregation may be accomplished by identification of a single order on one or more Purchase Orders. For the avoidance of doubt, two Agencies may purchase 5,000 Seat Subscriptions each and deliver Purchase Orders to DocuSign corresponding to their respective purchases; each Purchase Order may include notations that the Agencies aggregate their respective purchases.
 - c. Pricing tiers will be applied to each Agency's purchase by aggregating purchases pursuant to this Agreement made during each twelve month period of the initial term. For the avoidance of doubt, a purchase of Seat Subscriptions, or Envelope Allowance Subscriptions, will be priced at the cumulative number of Seats or Envelope Allowance comprising all previous purchases during a twelve month period.
4. The OSC and DocuSign will participate in joint marketing activity, to include press releases and other public promotional events.
 - a. Technology Day - From the beginning, DocuSign will engage in regularly scheduled "**Technology Day" sessions, demonstrations and presentations with support and guidance of the State Controller's office. Technology days will be scaled to accommodate the individual requirements of the attending participants. OSC will provide program and project oversight,

coordination with the agencies and conferences, scheduling locations for training, and assist with participant registration.

5. DocuSign and OSC will participate in periodic reviews of the Services, participating Agencies' uses of the Services, prospective uses by Agencies and implementation of the Services. Such reviews will be held at least quarterly during the initial Term. The Parties agree to engage in good faith discussions regarding renewal of the contract during the 5th or 6th quarterly review, and further agree that OSC may initiate such discussions at an earlier quarterly review in its discretion. The Parties agree to engage in good faith discussions regarding cost efficiencies, pricing and related topics during the 4th or 5th quarterly review, and further agree that OSC may initiate such discussions at an earlier quarterly review in its discretion.
 - a. DocuSign will schedule Quarterly business reviews with the State Controller's Office. Business Plan will include a Communications Plan, Conference Schedules, Platform updates and other programmatic offerings and new features and innovations as they become available.
 - b. DocuSign INK -DocuSign Ink may be used to increase adoption, citizen familiarity and trust around the State's selected eSign platform. DocuSign will work closely with the OSC to promote and support broad adoption of DocuSign's Freemium offering through the State of North Carolina. OSC will have the ability to offer constituents direct access to DocuSign INK through State operated web pages and portals.
 - c. eNotary - DocuSign will be providing a robust and well vetted solution for the State's eNotary initiative in the coming year. This will be a road mapped functionality of the DocuSign multi-tenant platform, and not custom development specifically for use by the State of North Carolina. As such, there will be no development cost to the State, or any required or allow feature acceptance testing or Signoff.
 - d. API – The DocuSign API is a standard capability for the platform, and will carry no on-going access fees. Each new implementation will require API certification, a process included in the Best Practice Fast Start Implementation Integrations. Certification processes that occur independent of the Best Practice Fast Start Implementation Integration packages will carry a fee of \$5,000 per certification.
6. Agencies may engage DocuSign for Professional Services as described in DocuSign's response to the RFP. In the event Agencies wish to obtain such Professional Services, an Agency will issue a Statement of Work (SOW) describing the Professional Services to be performed. SOWs shall be limited to the purposes of the contract, and shall be subject to the terms of this document.
 - a. Professional Services – The ad-hoc rate for Professional Services is \$295 per hour. Bundled Hourly rates can be as low as \$195 per hour, provided that the Agency's purchase is more than 40 hours.
7. DocuSign's API supports interoperation of applications with the Hosted Services and shall be maintained as compatible with all certified applications implemented by an Agency during the term of this Agreement, provided that DocuSign will provide six (6) months advance written notice to Agencies if any changes to the DocuSign API do not maintain backward compatibility with integrated, certified applications, and further, DocuSign shall provide any re-certifications required as a result of such changes at no charge to the Agencies.

Table 1 Envelope Allowance Subscriptions

Total number of Envelopes purchased by the State through all Envelope Allowance Subscriptions over the preceding twelve (12) months; including the Envelope Allowance Subscription purchase by OSC in the initial Purchase Order.	Envelope Factor (multiplied by number of Envelopes purchased in each Envelope Allowance Subscription)
10,000 – 49,999	\$0.55
50,000 -99,999	\$0.50
100,000 – 249,999	\$0.48
250,000 – 499,000	\$0.475
500,000 – 749,999	\$0.46
750,000 – 999,999	\$0.45
1,000,000 and above	\$0.43

Table 2 Seat Subscriptions

Volume of Seat Subscriptions purchased	Price
1 - 99	\$125 annually/Seat
100 – 249	\$120 annually/Seat
250 – 499	\$110 annually/Seat
500 – 999	\$100 annually/Seat
1000 – 4999	\$90 annually/Seat
5000 Seats and above	\$80 annually/Seat

The following amendments are made to the RFP:

Section II. Bidding Information

B. General Conditions for Proposals

7) Contract Term. A contract awarded pursuant to this RFP shall have an effective date as provided in the Notice of Award. The term of the contract shall be two (2) years, and will expire upon the anniversary date of the effective date unless otherwise stated in the Notice of Award, or unless terminated earlier. The State retains the option to extend the contract for additional periods at its sole discretion: renewals may be for a like term of two (2) years or a lesser term. Evaluations will be conducted not less than annually prior to the anniversary date to determine contract renewal(s).

Section VI. Other Specifications and Special Terms

- 1) VENDOR UTILIZATION OF WORKERS OUTSIDE U.S.: In accordance with NC General Statute 147-33.97, the Vendor must detail in the bid response, the manner in which it intends to utilize resources or workers. The State of North Carolina will evaluate the additional risks, costs, and other factors associated with such utilization prior to making an award for any such Vendor's proposal. The Vendor shall provide the following for any proposal or actual utilization or contract performance:
- a) The location of work performed under a state contract by the Vendor, any subcontractors, employees, or other persons performing the contract and whether any of this work will be performed outside the United States
 - b) The corporate structure and location of corporate employees and activities of the Vendors, its affiliates or any other subcontractors
 - c) Notice of the relocation of the Vendor, employees of the Vendor, subcontractors of the Vendor, or other persons performing services under a state contract outside of the United States
 - d) Any Vendor or subcontractor providing call or contact center services to the State of North Carolina shall disclose to inbound callers the location from which the call or contact center services are being provided

Will any work under this contract be performed outside the United States?

YES X NO _____

Where will services be performed: Tier 1 Customer Support Call Center is in Cebu City, Philippines (subcontractor)

- 2) Special Terms and Conditions –
- a) Paragraph #28 of the State's General Terms and Conditions for Goods and Related Services is superseded as follows: The State interprets the phrase "contract value" under this Paragraph to mean that liability shall be calculated on the basis of each Statement of Work and not on the estimated or cumulative value of the contract as a whole.
- 3) Financial Statements - The Vendor shall provide evidence of financial stability with its response to this RFP as further described herein below. As used herein, Financial Statements shall exclude tax returns and compiled statements.
- a) For a publicly traded company, Financial Statements for the past three (3) fiscal years, including at a minimum, income statements, balance sheets, and statement of changes in financial position or cash flows. If three (3) years of financial statements are not available, this information shall be provided to the fullest extent possible, but not less than one year. If less than 3 years, vendor must explain the reason why they are not available.
 - b) For a privately held company, when certified audited financial statements are not prepared: a written statement from the company's certified public accountant stating the financial condition, debt-to-asset ratio for the past three (3) years and any pending actions that may affect the company's financial condition.
 - c) The State may, in its sole discretion, accept evidence of financial stability other than Financial Statements for the purpose of evaluating Vendors' responses to this RFP. The State reserves the right to determine whether the substitute information meets the requirements for Financial Information sufficiently to allow the State to evaluate the sufficiency of financial resources and the ability of the business to sustain performance of the contract award. Scope Statements issued may require the

submission of Financial Statements and specify the number of years to be provided, the information to be provided, and the most recent date required.

- 4) Disclosure of Litigation – The Vendor's failure to fully and timely comply with the terms of this section, including providing reasonable assurances satisfactory to the State, may constitute a material breach of this Contract.
- a) The Vendor shall notify the State in its bid proposal, if it, or any of its subcontractors, or their officers, directors, or key personnel who may provide services under any contract awarded pursuant to this solicitation, have ever been convicted of a felony, or any crime involving moral turpitude, including, but not limited to fraud, misappropriation or deception. Vendor shall promptly notify the State of any criminal litigation, investigations or proceeding involving Vendor or any subcontractor, or any of the foregoing entities' then current officers or directors during the term of this Contract or any Scope Statement awarded to Vendor.
 - b) Vendor shall notify the State in its bid proposal, and promptly thereafter as otherwise applicable, of any civil litigation, arbitration, proceeding, or judgments against it or its subcontractors during the three (3) years preceding its bid proposal, or which may occur during the term of any awarded to Vendor pursuant to this solicitation, that involve (1) services or related goods similar to those provided pursuant to any contract and that involve a claim that may affect the viability or financial stability of the Vendor, or (2) a claim or written allegation of fraud by the Vendor or any subcontractor hereunder, arising out of their business activities, or (3) a claim or written allegation that the Vendor or any subcontractor hereunder violated any federal, state or local statute, regulation or ordinance. Multiple lawsuits and or judgments against the Vendor or subcontractor shall be disclosed to the State to the extent they affect the financial solvency and integrity of the Vendor or subcontractor.
 - i) DocuSign became the defendant in a lawsuit filed June 24, 2011, in the Eastern District of Texas by Rmail Ltd., Rmail Communications Ltd, and Rpost Holdings, Inc., alleging patent infringement and seeking unspecified damages. In its July 29, 2011 answer and motion for transfer, DocuSign responded that we do not infringe and have not infringed on any of the asserted patent claims. As this is a pending legal matter, DocuSign can offer no further comment.
 - c) All notices under subsection A and B herein shall be provided in writing to the State within thirty (30) calendar days after the Vendor learns about any such criminal or civil matters; unless such matters are governed by the ITS General Terms and Conditions annexed to the solicitation. Details of settlements which are prevented from disclosure by the terms of the settlement shall be annotated as such. Vendor may rely on good faith certifications of its subcontractors addressing the foregoing, which certifications shall be available for inspection at the option of the State.
- 5) Criminal Conviction – In the event the Vendor, an officer of the Vendor, or an owner of a 25% or greater share of the Vendor, is convicted of a criminal offense incident to the application for or performance of a State, public or private Contract or subcontract; or convicted of a criminal offense including but not limited to any of the following: embezzlement, theft, forgery, bribery, falsification or destruction of records, receiving stolen property, attempting to influence a public employee to breach the ethical conduct standards for State of North Carolina employees; convicted under State or federal antitrust statutes; or convicted of any other criminal offense which in the sole discretion of the State, reflects upon the Vendor's business integrity and such vendor shall be prohibited from entering into a contract for goods or services with any department, institution or agency of the State.
- 6) Security and Background Checks – The Agency reserves the right to conduct a security background check or otherwise approve any employee or agent provided by Vendor, and to refuse access to or require replacement of any such personnel for cause, including, but not limited to, technical or training qualifications, quality of work or change in security status or non-compliance with the Agency's security or other requirements.

- 7) Assurances – In the event that criminal or civil investigation, litigation, arbitration or other proceedings disclosed to the State pursuant to this Section, or of which the State otherwise becomes aware, during the term of this Contract, causes the State to be reasonably concerned about:
- a) the ability of the Vendor or its subcontractor to continue to perform this Contract in accordance with its terms and conditions, or
 - b) whether the Vendor or its subcontractor in performing services is engaged in conduct which is similar in nature to conduct alleged in such investigation, litigation, arbitration or other proceedings, which conduct would constitute a breach of this Contract or violation of law, regulation or public policy, then the Vendor shall be required to provide the State all reasonable assurances requested by the State to demonstrate that: the Vendor or its subcontractors hereunder will be able to continue to perform this Contract in accordance with its terms and conditions, and the Vendor or its subcontractors will not engage in conduct in performing services under this Contract which is similar in nature to the conduct alleged in any such litigation, arbitration or other proceedings.
- 8) Security Audit. Upon thirty (30) business days' notice to Vendor, an independent third party auditor mutually acceptable to both Parties will have the right to conduct an on-site audit of the System on behalf of Customer and at Customer's sole expense during Vendor's normal business hours to verify that Vendor is in compliance with any security obligations under this Agreement. The auditor must sign a confidentiality agreement with Vendor and comply with Vendor's security rules, policies, and procedures. Vendor shall cooperate with the auditor by: (i) making applicable records available, (ii) providing copies of the records requested, and (iii) directing Vendor employees to cooperate.
- 9) Confidentiality of Data and Information –All financial, statistical, personnel, technical and other data and information relating to the State's operation which are designated confidential by the State and made available to the Vendor in order to carry out this Contract, or which become available to the Vendor in carrying out this Contract, shall be protected by the Vendor from unauthorized use and disclosure through the observance of the same or more effective procedural requirements as are applicable to the State. The identification of all such confidential data and information as well as the State's procedural requirements for protection of such data and information from unauthorized use and disclosure shall be provided by the State in writing to the Vendor. If the methods and procedures employed by the Vendor for the protection of the Vendor's data and information are deemed by the State to be adequate for the protection of the State's confidential information, such methods and procedures may be used, with the written consent of the State, to carry out the intent of this section. The Vendor shall not be required under the provisions of this section to keep confidential, (1) information generally available to the public, (2) information released by the State generally, or to the Vendor without restriction, (3) information independently developed or acquired by the Vendor or its personnel without reliance in any way on otherwise protected information of the State. Notwithstanding the foregoing restrictions, the Vendor and its personnel may use and disclose any information which it is otherwise required by law to disclose, but in each case only after the State has been so notified, and has had the opportunity, if possible, to obtain reasonable protection for such information in connection with such disclosure.
- a) Protection of Personal Identifying Information. Vendor acknowledges its responsibility for securing personal identifying information collected by the State and stored in any Vendor site or other Vendor housing systems, including but not limited to computer systems, networks, servers, or databases, maintained by Vendor or its agents or subcontractors in connection with the System or Services. Vendor warrants, at its sole cost and expense, that it shall implement processes and maintain security of personal identifying information; provide reasonable care and efforts to detect fraudulent activity involving personal identifying information; and promptly notify the Agency of any breaches of security involving personal identifying information.
 - b) Vendor shall operate and maintain the Software and System described herein and in its published materials in good working order with access restricted to qualified employees and affiliates of, and contractors designated by, Vendor. Vendor shall undertake and perform commercially reasonable measures designed to protect the security, confidentiality, and integrity of State data and other

information, including firewall protection and maintenance of independent archival and backup copies of such data and information collected or received by Vendor. Except as otherwise agreed, Vendor will not disclose State data or other information to third-parties except in response to a subpoena or Court order, to report a criminal offense, or otherwise as may be required by law; and only upon prior notification to the State and affected Agency.

- c) All Vendor project team members who have access to non-public State data must sign the confidentiality agreement satisfactory to the Agency disclosing the State data.
- d) Vendor agrees not to release any State data, whether it is confidential or not, unless authorized by Customer or otherwise as required by law. Vendor shall return all State data, including all Personal Identifying Information, to the State at the expiration or termination of this Agreement in a reasonably accessible format and shall keep no copies in any form or format. Notwithstanding the foregoing or anything to the contrary this contract or any subsequent agreement between the parties, Vendor shall not be required to expunge or destroy Transaction Data. "Transaction Data" is defined as data associated with an electronic contract or document, including transaction history, the image hash value of such electronic contract or document, information concerning method and time of electronic contract purge, and sender and recipient names, email addresses and signature IDs.
- e) **LIABILITY FOR DISCLOSING CONFIDENTIAL INFORMATION.** Vendor will indemnify and hold harmless the State from all losses, damages, costs or reasonable attorneys' fees incurred by the State or any of its agents or employees, for which Vendor is liable arising out of a breach of this Section by Vendor, its employees or agents.

10) **Security Breach.** "Security Breach" means (1) any circumstance pursuant to which applicable Law requires notification of such breach to be given to affected parties or other activity in response to such circumstance; or (2) any actual, attempted, suspected, threatened, or reasonably foreseeable circumstance that compromises, or could reasonably be expected to compromise either physical security or systems security in a fashion that either does or could reasonably be expected to permit unauthorized processing, use, disclosure or acquisition of or access to any Agency data or Agency or User confidential information. In the event Vendor becomes aware of any Security breach, Vendor shall, at its own expense, (1) immediately notify the Agency's Contract Administrator of such security breach and perform a root cause analysis thereon, (2) investigate such security breach, (3) provide a remediation plan, acceptable to the Agency, to address the security Breach and prevent any further incidents, (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (5) cooperate with the Agency, and any law enforcement or regulatory officials investigating such Security Breach. The Agency shall make the final decision on notifying the Agency's persons, entities, employees, service providers and/or the general public of such Security Breach ("Notification"), and the implementation of the remediation plan unless Vendor is required by law to perform such Notification independently from the Agency. If a Notification to a customer is required under any Law, or pursuant to any of the State's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by the Agency) shall be considered legally required. Vendor shall reimburse the Agency for all Notification Related Costs incurred by the Agency arising out of or in connection with any such Security Breach.

- a) **Breach Notification.** In the event Vendor becomes aware of any Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Contract, Vendor shall, at its own expense, (1) immediately notify the State's Contract Administrator of such Security Breach and perform a root cause analysis thereon, (2) investigate such Security Breach, (3) provide a remediation plan, acceptable to the State, to address the Security Breach and prevent any further incidents, (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (5) cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach. The State shall make the final decision on notifying the State's persons, entities, employees, service providers and/or the general public of such Security Breach, and the implementation of the remediation plan unless Vendor is

required by law to perform such Notification independently from the Agency. If a notification to a customer is required under any Law or pursuant to any of the State's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by the State) shall be considered legally required.

- b) Notification Related Costs. Vendor shall reimburse the State for all Notification Related Costs incurred by the State arising out of or in connection with any such Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Contract resulting in a requirement for legally required notifications. "Notification Related Costs" shall include the State's internal and external costs associated with addressing and responding to the Security Breach, including but not limited to: (1) preparation and mailing or other transmission of legally required notifications; (2) preparation and mailing or other transmission of such other communications to customers, agents or others as the State deems reasonably appropriate; (3) establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training); (4) public relations and other similar crisis management services; (5) legal and accounting fees and expenses associated with the State's investigation of and response to such event; and (6) costs for credit reporting services that are associated with legally required notifications or are advisable, in the State's opinion, under the circumstances. In the event that Vendor becomes aware of any Security Breach which is not due to Vendor acts or omissions other than in accordance with the terms of the Contract, Vendor shall immediately notify the State of such Security Breach, and the parties shall reasonably cooperate regarding which of the foregoing or other activities may be appropriate under the circumstances, including any applicable Charges for the same.
- 11) Agency Data. Vendor shall not withhold the Agency Data or any other Agency Confidential Information or refuse for any reason (including due to the Agency's actual or alleged breach of the Contract) to promptly return to the Agency the Agency Data and any other Agency confidential information (including copies thereof) if requested to do so on such media as reasonably requested by the Agency, even if the Agency is then or is alleged to be in breach of the Contract. As a part of Vendor's obligation to provide the Agency Data pursuant to this Section, Vendor will also provide the Agency any data maps, documentation, software, or other materials necessary, including, without limitation, handwritten notes, materials, working papers or documentation, for the Agency to use, translate, interpret, extract and convert the Agency Data and any other Agency Confidential Information for use by the Agency or any third party.
- 12) Project Management – All project management and coordination on behalf of the Agency shall be through a single point of contact designated as the Agency Project Manager. Vendor shall designate a Vendor Project Manager who will provide a single point of contact for management and coordination of Vendor's work. All work performed pursuant to this Contract shall be coordinated between the Agency Project Manager and the Vendor Project Manager.
- 13) Meetings – The Vendor is required to meet with Agency personnel, or designated representatives, to resolve technical or contractual problems that may occur during the term of the Contract. Meetings will occur as problems arise and will be coordinated by Agency. The Vendor will be given reasonable and sufficient notice of meeting dates, times, and locations. Face to face meetings are desired. However, at the Vendor's option and expense, a conference call meeting may be substituted. Consistent failure to participate in problem resolution meetings, two (2) consecutive missed or rescheduled meetings, or failure to make a good faith effort to resolve problems, may result in termination of the Contract.
- 14) Transition Assistance – If this Contract is not renewed at the end of this term, or is canceled prior to its expiration, for any reason, the Vendor must provide for up to twelve (12) months after the expiration or cancellation of this Contract, all reasonable transition assistance requested by the State, to allow for the expired or canceled portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such services to the State or its designees. Such transition assistance will be deemed by the parties to be governed by the terms and conditions of this Contract, (notwithstanding this expiration or cancellation) except for those Contract terms or conditions that do not reasonably apply to such transition assistance. The State shall pay the Vendor for any Services or resources utilized in

performing such transition assistance at the most current rates provided by the Contract for Contract performance. If the State cancels this Contract for cause, then the State will be entitled to off set the cost of paying the Vendor for the additional resources the Vendor utilized in providing transition assistance with any damages the State may have otherwise accrued as a result of said cancellation.

- 15) Unanticipated Tasks – In the event that additional work must be performed that was wholly unanticipated, and that is not specified in this Contract, but which in the opinion of both parties is necessary to the successful accomplishment of the contracted scope of work, the procedures outlined in this article will be followed. For each item of unanticipated work, Vendor shall prepare a work authorization in accordance with the State's practices and procedures.
- a) It is understood and agreed by both parties that all of the terms and conditions of this Contract shall remain in force with the inclusion of any work authorization. A work authorization shall not constitute a contract separate from this Contract, nor in any manner amend or supersede any of the other terms or provisions of this Contract or any amendment hereto.
 - b) Each work authorization shall comprise a detailed statement of the purpose, objective, or goals to be undertaken by Vendor, the job classification or approximate skill level or sets of the personnel required, an identification of all significant material then known to be developed by Vendor's personnel as a Deliverable, an identification of all significant materials to be delivered by the State to Vendor's personnel, an estimated time schedule for the provision of the services by Vendor, completion criteria for the work to be performed, the name or identification of Vendor's personnel to be assigned, the Vendor's estimated work hours required to accomplish the purpose, objective or goals, the Vendor's billing rates and units billed, and the Vendor's total estimated cost of the work authorization.
 - c) All work authorizations must be submitted for review and approval by the procurement office that approved the original Contract and procurement. This submission and approval must be completed prior to execution of any work authorization documentation or performance there under. All work authorizations must be written and signed by Vendor and the State prior to beginning work.
 - d) The State has the right to require Vendor to stop or suspend performance under the "Stop Work" provision of the General Terms and Conditions for Goods and Related Services.
 - e) Vendor shall not expend Personnel resources at any cost to the State in excess of the estimated work hours unless this procedure is followed: If, during performance of the work, the Vendor determines that a work authorization to be performed under this Contract cannot be accomplished within the estimated work hours, the Vendor will be required to complete the work authorization in full. Upon receipt of such notification, the State may:
 - i.) Authorize the Vendor to expend the estimated additional work hours or service in excess of the original estimate necessary to accomplish the work authorization, or
 - ii.) Terminate the work authorization, or
 - iii.) Alter the scope of the work authorization in order to define tasks that can be accomplished within the remaining estimated work hours.
 - iv.) The State will notify Vendor in writing of its election within seven (7) calendar days after receipt of the Vendor's notification. If notice of the election is given to proceed, the Vendor may expend the estimated additional work hours or services.

Section VIII. North Carolina Information Technology Procurement Office General Terms and Conditions for Goods and Related Services

Definitions: As used herein;

"Account" means a unique account established by an Agency in order to gain access for its Authorized Users to the Software and, where applicable, other DocuSign Products.

"Authorized User" means an individual employee or third party agent, as identified by a unique email address and user name, who is registered as a member of Agency's Account. No two persons may register, access or use the Software as the same Authorized User.

"Professional Services" means those additional Vendor services, including training, consulting, and custom development, if any, that are made the subject of a Purchase Order or statement of work.

"Depositing Party" refers to an Authorized User that deposits a document into the System for Processing under the Software.

"DocuSign API" means Vendor's application programming interface that supports interoperation of applications with the Software.

"DocuSign Products" means the products and services identified on a Purchase Order, including, but not limited to, the Software and, where applicable, Consulting Services.

"eContract" refers to a contract, notice, disclosure, or other record or document deposited into the System by a Depositing Party for Processing under the Software.

"Envelope" means an electronic record containing one or more eContracts consisting of a single page or a group of pages of data uploaded to the System.

"Order Term" means the length of the subscription purchased by an Agency pursuant to a Purchase Order, starting on the Order Start Date and continuing for the term specified on the Purchase Order.

"Purchase Order" means a purchase order or any other document that describes DocuSign Products to be purchased by an Agency, that is issued through the State's E-Procurement System, and that is based on the mutually agreed upon terms of this Agreement.

"Process" and similar terms mean to perform any operation or set of operations upon State Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, accessing, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Specifications" means the Software Specifications available at <http://docusign.com/support/specifications.php>.

"State" shall mean the State of North Carolina, the Office of Information Technology Services as an Agency or in its capacity as the Award Authority.

"Purchasing State Agency or Agency" shall mean the Agency purchasing the goods or services.

"State Data" means the following, whether provided or produced before, on or after the Contract Effective Date:

- all taxpayer data, information, and material, by whatever name known, collected, processed and stored pursuant to Agency's statutory and regulatory powers;

- all information and data (copyrighted or otherwise) developed, derived, documented, or stored by Agency under the Contract;

- all data that is provided by or on behalf of Agency to Vendor in order for Vendor to provide the Services or Deliverables pursuant to the Contract;

all records, files, reports and other data provided to Vendor by or on behalf of Agency, or otherwise collected or obtained by Vendor, in connection with the Services or Deliverables; and

all data that is produced as an intermediate step in using or producing any of the State Data, including databases and files containing the State Data.

Notwithstanding the foregoing definition of State Data or anything to the contrary in this contract or any subsequent agreement between the parties, Vendor's Transaction Data shall not be considered part of the definition of State Data other than sender and recipient names, email addresses.

For purposes of this RFP and any resulting Contract, "Services" shall mean the services and Deliverables (including, without limitation, the hardware, software, tangibles, and intangibles required hereunder) to be delivered by Vendor pursuant to the Contract, including, without limitation, the Inherent Services described in Section II, 1).

"Software" or "Software Application" shall mean the Web-based Software Application, i.e. SaaS provided by the Vendor under this solicitation.

"System" refers to the software systems and programs, communication and network facilities, and hardware and equipment used by DocuSign or its agents to provide the Software.

"Transaction Data" means data associated with an eContract, including transaction history, eContract image hash value, information concerning method and time of eContract purge, and sender and recipient names, email addresses and signature IDs.

1) Standards: Manufactured items and/or fabricated assemblies comprising Deliverables shall meet all requirements of the Occupational Safety and Health Act (OSHA), and State and federal requirements relating to clean air and water pollution, if applicable. Vendor will provide and maintain a quality assurance system or program that includes any Deliverables and will tender to the State only those Deliverables that have been inspected and found to conform to the requirements of this Contract. All manufactured items and/or fabricated assemblies comprising Deliverables are subject to operation, certification or inspection, and accessibility requirements as required by:

- State or Federal Regulation,
 - The Chief Information Officer's (CIO) policy or regulation, or
 - Acceptance with appropriate standards of operations or uses of said Deliverables as may be shown by identification markings or other means of the appropriate certifying standards organization.
- a) **Site Preparation:** Vendors shall provide the Purchasing State Agency complete site specifications for the Deliverables, if any. These specifications shall ensure that the Deliverables to be installed shall operate properly and efficiently within the site environment. The Vendor shall advise the State of any site requirements for any Deliverables required by the State's specifications. Any alterations or modification in site preparation which are directly attributable to incomplete or erroneous specifications provided by the Vendor and which would involve additional expenses to the State, shall be made at the expense of the Vendor.
 - b) Reserved
 - c) **Specifications:** The apparent silence of the specifications as to any detail, or the apparent omission of detailed description concerning any Deliverables, shall be regarded as meaning that only the best commercial practice is to prevail and only material and workmanship of the first quality may be used in producing the Deliverables. Upon any notice of noncompliance provided by the State, Vendor shall supply proof of compliance with the specifications. Vendor must provide written notice of its intent to deliver alternate or substitute products, goods or Deliverables. Alternate or substitute products, goods or Deliverables may be accepted or rejected in the sole discretion of the State; and any such alternates or substitutes must be accompanied by Vendor's certification and evidence satisfactory to the State

that the function, characteristics, performance and endurance will be equal or superior to the original Deliverables specified.

- d) **Pre-Contractual Expenses:** The State shall not, in any event, be liable for any pre-contractual expenses incurred by a Vendor in the preparation of its Proposal(s). Vendor shall not include any such expenses as part of its Proposal(s), nor as a claim in any bid protest or other proceeding against the State. Pre-contractual expenses are defined as expenses incurred by the Vendor in preparing its response to this RFP; submitting that Proposal to the State; negotiating with the State any matter related to this RFP or any Proposal; and, any other expenses incurred by the Vendor prior to, or following, the date of award, and execution of an Agreement.

2) Warranties: The Vendor warrants to the State that all Deliverables furnished will be new (unless otherwise requested in this bid), of good material and workmanship, and agrees to replace any items which fail to comply with the specifications by reason of defective material or workmanship under normal use, free of State's negligence or accident for a minimum of 90 days from date of acceptance. Such replacement shall include transportation costs free of any charge to the State. This statement is not intended to limit any additional coverage, which may normally be associated with a product. Vendor shall assign all applicable third party warranties for Deliverables to the Purchasing State Agency.

3) Personnel: Vendor shall not substitute key personnel assigned to the performance of this Contract without prior written approval by the Agency Contract Administrator. Any desired substitution shall be noticed to the Agency's Contract Administrator accompanied by the names and references of Vendor's recommended substitute personnel. The Agency will approve or disapprove the requested substitution in a timely manner. The Agency may, in its sole discretion, terminate the services of any person providing services under this Contract. Upon such termination, the Agency may request acceptable substitute personnel or terminate the contract services provided by such personnel.

a) Vendor personnel shall perform their duties on the premises of the State, during the State's regular work days and normal work hours, except as may be specifically agreed otherwise, established in the specification, or statement of work.

b) This contract shall not prevent Vendor or any of its personnel supplied under this Contract from performing similar services elsewhere or restrict Vendor from using the personnel provided to the State, provided that:

- i) Such use does not conflict with the terms, specifications or any amendments to this Contract, or
- ii) Such use does not conflict with any procurement law, regulation or policy or
- iii) Such use does not conflict with any non-disclosure agreement, or term thereof, by and between the State and Vendor or Vendor's personnel.

4) Subcontracting: The Vendor may subcontract the performance of required services with other Vendors or third parties provided that Vendor notifies the State in writing in advance concerning its use of any such subcontractor, or and agrees that for any change to or addition of such subcontractors, will do so only with the prior written consent of the contracting authority. Vendor hereby notifies the State that it utilizes the subcontractors listed in subsection a) below to perform certain material services supporting Vendor's provision of the Software to the State hereunder. Subject to confidentiality, personnel privacy and other similar legal and regulatory obligations with which Vendor must comply, Vendor shall use all commercially reasonable efforts to obtain the applicable subcontractors' consent or any other actions necessary to permit Vendor to provide the State with complete copies of any agreements made by and between Vendor and all subcontractors upon the State's reasonable requests therefor. The selected Vendor remains solely responsible for the performance of its subcontractors. Subcontractors, if any, shall adhere to the same standards required of the selected Vendor. Following the Effective Date of this Agreement, any contracts made by the Vendor with a subcontractor shall include an affirmative statement that the State is an intended third party beneficiary of the contract; that the subcontractor has no agreement with the State; and that the State shall be indemnified by the Vendor for any claim presented by the subcontractor. Notwithstanding any other term herein, Vendor shall timely exercise its

contractual remedies against any non-performing subcontractor and, when appropriate, substitute another subcontractor.

a) Vendor's Current Subcontractors List:

i) **Data Centers:**

(1) Savvis, Inc.

Corporate address: 1 Savvis Parkway, Town & Country, MO 63017

Services locations:

12301 Tukwila International Blvd., Tukwila, WA 98168

350 E Cermak, Chicago, IL 60616

(2) Sungard Availability Services LP

Corporate address: 680 East Swedesford Road, Wayne, Pennsylvania 19087

Services location: 1001 East Campbell Road, Richardson, TX 75081-1821

ii) **ID Check (Knowledge-based authentication):**

(1) RSA Security LLC

Corporate address: 1550 Sawgrass Corporate Parkway, Suite 200, Ft. Lauderdale, FL 33323

Services location: (not applicable)

iii) **Phone Authentication:**

(1) Authentify, Inc.

Corporate address: 8745 West Higgins Road, Suite 240, Chicago, Illinois 60631

Services location: (not applicable)

iv) **Tier 1 Customer Support Call Center:**

(1) SupportSave Solutions, Inc.

Corporate address: 11132 Ventura Blvd, Suite 420, Studio City, CA 91604

Services location: Cebu City, Philippines

v) **Fax-back Service:**

(1) EasyLink International Services Corporation

Corporate address: 6025 The Corners Parkway, Suite 100, Norcross, GA 30092

Services location: (not applicable)

5) Vendor's Representation: Vendor warrants that qualified personnel will provide services in a professional manner. "Professional manner" means that the personnel performing the services will possess the skill and competence consistent with the prevailing business standards in the information technology industry. Vendor agrees that it will not enter any agreement with a third party that might abridge any rights of the State under this Contract. Vendor will serve as the prime Vendor under this Contract. Should the Vendor utilize any subcontractor(s), the Vendor shall be legally responsible for the performance and payment of the subcontractor(s). Names of any third party Vendors or subcontractors of Vendor may appear for purposes of convenience in Contract documents; and shall not limit Vendor's obligations hereunder. Third party subcontractors, if approved, may serve as subcontractors to Vendor. Vendor will retain executive representation for functional and technical expertise as needed in order to incorporate any work by third party subcontractor(s).

a) Good Faith Response, Reasonable Execution. Vendor acknowledges that prior to the Effective Date, Vendor received or had access to all information which it deemed necessary for Vendor to respond in good faith to the RFP and, to its knowledge, Vendor has requested and received all information it deems necessary to cause its execution of the Contract to be appropriately informed and undertaken reasonably. Vendor does not, to its knowledge, lack any information or know of any state of affairs or circumstances with respect to the Procurement Library, the information contained or not contained therein, or the activities proposed or not proposed therein, that cause Vendor to anticipate requesting any amendments to the Contract after its execution. As of the Effective Date, Vendor has no knowledge of facts or circumstances which would cause it to request an amendment to the Contract and knows of no information it does not

have, the presence of which could reasonably be expected to cause it to request an amendment to the Contract.

b) Intellectual Property. Vendor has the right to provide the Services and Deliverables without violating or infringing any law, rule, regulation, copyright, patent, trade secret or other proprietary right of any third party. Except as otherwise stated in Section VI.3)b) of the Specifications and Special Terms, Vendor represents that its Services and Deliverables are not the subject of any actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party.

c) Inherent Services. If any Services, Deliverables, functions, or responsibilities not specifically described in this Contract are required for Vendor's proper performance, provision and delivery of the Service and Deliverables pursuant to this Contract, or are an inherent part of or necessary sub-task included within the Service, they will be deemed to be implied by and included within the scope of the Contract to the same extent and in the same manner as if specifically described in the Contract. Unless otherwise expressly provided in the Contract, Vendor will furnish all of its own necessary management, supervision, labor, facilities, furniture, computer and telecommunications equipment, software, supplies and materials necessary for the Vendor to provide and deliver the Services and Deliverables.

d) A contract or transaction otherwise enforceable under the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001 et seq. will not be denied legal effect, validity, or enforceability solely because Vendor's Software and System enabling electronic signatures were used in its formation.

e) Technology. Vendor will keep knowledgeable about changes and advancements over time in the technology necessary to provide the Services. In performing the Services, Vendor will utilize processes, procedures and practices that are no less effective than the practices it utilizes in performing services similar to the Services for its other customers, which practices will, at a minimum, be no less effective than the practices of similarly situated providers offering similar services within the digital signature industry at this time.

f) Viruses. Vendor will screen any software or data files provided or made available by it to the Agency hereunder or used by Vendor (or any Vendor agent, contractor, subcontractor or representative) in performance of the Services or providing Deliverables and will use then-current industry-standard anti-virus software programs for the purpose of avoiding the introduction of any "virus" or other computer software routine or hardware components which are designed to disable or damage hardware or damage, erase or delay access to software or data. Vendor will assist the Agency's recovery from the introduction of any such virus.

g) Vendor warrants that it has the financial capacity to perform and to continue to perform its obligations under the Contract; that Vendor has no constructive or actual knowledge of any pending or threatened action, proceeding, or investigation, or any other legal action, that would in any way prohibit, restrain, or diminish Vendor ability to satisfy its contractual obligations hereunder; and that entering into this Contract is not prohibited by any contract, or order by any court of competent jurisdiction.

h) Warranty as to Equipment; Hardware. Vendor warrants that the equipment and hardware that it provides pursuant to this Contract shall be free from defects in materials, in good working order and be maintained in good working order.

i) Vendor agrees to use commercially reasonable efforts to provide the Software and System twenty-four (24) hours a day, seven (7) days a week. User agrees that from time to time the Software and System may be inaccessible or inoperable for various reasons, including periodic maintenance procedures or upgrades ("Scheduled Downtime"); network or service malfunctions; and causes beyond the control of Vendor or which are not reasonably foreseeable by Vendor, including the interruption or failure of telecommunication or digital transmission links, hostile network attacks or network congestion or other failures (collectively "Downtime"). Vendor will provide at least forty-eight (48) hours notice to User in the event of any Scheduled Downtime. Scheduled downtime must be outside of regular business hours (Monday – Friday, 7:00am – 7:00pm EST). Notification should at a minimum include email, posting on website and phone call to Agency Service desk. Vendor agrees to use commercially reasonable efforts to minimize any disruption,

inaccessibility and/or inoperability of the Software and System in connection with Downtime, whether scheduled or not.

6) Software: From the Order Start Date defined in the applicable Purchase Order, an Agency may obtain an Account and register Authorized Users, and subject to these terms, such Authorized Users may log onto and use the Software in accordance with the Specifications. Agency's right to use the Software is limited to its Authorized Users, and Agency agrees not to resell or otherwise provide or assist with the provision of the Software to any other third party. Use of the Software by Agency and its Authorized Users is subject to Agency's acknowledgement and agreement that:

a) Nothing in this Agreement will be construed to make Vendor a party to any eContract, and Vendor makes no representation or warranty regarding the transactions sought to be effected by any eContract;

b) Vendor maintains no control or access to the contents of any eContract, and the content, quality, and format of any eContract is completely within the exclusive control of the Depositing Party and is the responsibility of Agency;

c) The Software may provide options, if Agency elects to purchase such options, designed to verify the identity of the intended recipient of an eContract deposited into the System ("Authentication Measures"), and Vendor: (i) will apply only those Authentication Measures (if any) selected by the Depositing Party; (ii) makes no representations or warranties regarding the appropriateness of such Authentication Measures; and (iii) assumes no liability or responsibility for a party's inability or failure to satisfy any particular Authentication Measure or for any circumvention of such Authentication Measures effected by any third party;

d) Certain types of agreements and documents are excepted from electronic signature laws, such that they cannot be legally formed by electronic signatures; additionally, various agencies may have promulgated specific regulations that apply to electronic signatures and electronic records, and Vendor assumes no responsibility to determine whether any particular eContract is an exception to applicable electronic signature laws or whether it is subject to any particular agency promulgations and whether it can be legally formed by electronic signatures;

e) Agency is solely responsible for making available to third parties (including parties to its eContracts) all contracts, documents, and other records required by applicable law, including, without limitation, electronic signature laws and other laws that may require records relating to a transaction to be retained or made accessible for a certain period of time; and

f) Certain laws or regulations may impose special requirements with respect to electronic transactions involving one or more "consumers." These may include, among other things, requirements that the consumer consent to the method of contracting and/or that the consumer be provided with a copy, or access to a copy, of a paper or other non-electronic, written record of the transaction. Vendor assumes no responsibility to determine whether any particular transaction involves a consumer, nor does Vendor have any responsibility: (i) to furnish or obtain any such consents or to determine if any such consents have been withdrawn; (ii) to provide any information or disclosures in connection with any attempt to obtain any such consents; (iii) to provide legal review of, or to update or correct any information or disclosures currently or previously given; (iv) to provide any such copies or access except as expressly provided in the Specifications for all transactions, consumer or otherwise; or (v) otherwise to comply with any such special requirements. Agency expressly undertakes to determine whether any consumer is involved in any eContract presented by Agency or its Authorized Users for Processing; and, if so, to comply with all requirements imposed by law on such eContracts or their formation.

g) Subscription Plans and Per Use Purchases. The price, features, and options of the DocuSign Products available for an Account depend on the level of service, features, and promotions selected by Agency pursuant to the Purchase Order. Use of the Software is sold on a subscription basis and may be limited by usage ("Envelope Allowance") or the number of Authorized Users ("Seats"), or both. Some optional services, such as ID check, may be purchased on a periodic or per-use basis.

h) Usage and Seats.

i) A Vendor Subscription based on Envelope Allowance allows Agency to send the number of Envelopes in the Envelope Allowance specified in the Purchase Order during the Order Term. All Envelopes sent in excess of the Envelope Allowance will incur a per-Envelope charge, at the Envelope Factor, that will be invoiced within 30 days of the date first incurred. The total number of Envelopes sent is calculated by the sum of all Envelopes that have been sent for signature or certified delivery. Envelopes may be sent to any number of recipients who may sign in any number of places within the contents of the sent Envelope. Agency's Account will be deemed to have consumed an Envelope at the time the Envelope is sent by Agency, regardless of whether Envelopes were received by recipients, or whether recipients have performed any actions upon any eContract in the Envelope.

ii) Vendor Subscription based on Seats allows Agency to send a reasonable number of Envelopes from the number of Seats specified in the Order Form during the Purchase Order. If Vendor suspects that the number of Envelopes sent from a particular Seat or a group of Seats is abusive and/or unduly burdensome (by way of example, bulk sending or processing automated batch operations), Vendor will promptly notify Agency, discuss the use-case scenario with Agency and any continued monitoring, additional discussions and/or information required to make a final determination on the course of action based on such information. The number of Seats is determined by the total number of active Authorized Users listed in the membership of an Account at any one time. No two individuals may log onto or use the Software as the same Authorized User, but Agency may unregister or deactivate Authorized Users and replace them with other Authorized Users without penalty, so long as the number of active Authorized Users registered at any one time is equal to or less than the number of Seats purchased. The addition by Agency of more Authorized Users than the number of Seats purchased in an Order Form will result in an additional charge for one Seat per additional Authorized User for the remainder of the Order Term, to be invoiced immediately. A Vendor Subscription based on Seats explicitly excludes use of the DocuSign API for sending Envelopes. As used herein, abusive and/or unduly burdensome use of a Seat Subscription shall not exclude reasonable use; and reasonable use refers to such use as an individual may perform in the ordinary course of their job duties, where such job duties do not entail generating large numbers of individual transactions grouped as mass mailings transaction documents for signatures.

iii) Per use charges are specific to the number of units of the DocuSign Product(s) used during the period, and are measured at the time of use.

i) Additional Agency Responsibilities.

i) Agency agrees that it will not use or permit the use of the Software to send unsolicited mass mailings outside its organization, it being understood that the term "unsolicited mass mailings" includes all statutory and other common definitions, including all Commercial Electronic Marketing Messages as defined in the U.S. CAN SPAM Act.

ii) Agency agrees that it is solely responsible for the nature and content of all materials, works, data, statements, and other visual, graphical, video, written or audible communications of any nature submitted by any Authorized User or otherwise Processed through Agency's Account.

iii) Agency further agrees not to use or permit the use of the Software: (a) to communicate any message or material that is defamatory, harassing, libelous, threatening, or obscene; (b) in a way that violates or infringes upon the intellectual property rights or the privacy or publicity rights of any person or entity or that may otherwise be unlawful or give rise to civil or criminal liability (other than contractual liability of the parties under eContracts Processed through the Software); (c) in any manner that is likely to damage, disable, overburden, or impair the System or the Software or interfere in any way with the use or enjoyment of the Software by others; or (d) in any way that constitutes or encourages conduct that could constitute a criminal offense. Although Vendor does not actively monitor the content Processed through the Software, Vendor may at any time and without prior notice suspend any use of the Software and/or remove or disable any content as to which Vendor is made aware of a reason for concern as to such use or content. Vendor agrees to exert reasonable commercial efforts to provide

Agency with notice of any such suspension or disablement before its implementation, or promptly thereafter.

j) Storage

i) General eContract Storage and Deletion Policy. Unless otherwise directed by Agency, Vendor will store in accordance with the Specifications all completed eContracts sent by Agency until the term of the Contract expires. Copies of stored eContracts may be retrieved by Agency at any time during the Term. After expiration or termination of the Term, Agency may request Vendor's assistance in retrieving completed eContracts still remaining on the System pursuant to the transition services terms described in Section 30)b). Prior to the expiration or termination of this Agreement, Agency may elect to purchase post-expiration or post-termination storage services for their completed eContracts. Where Agency opts not to purchase storage services, all copies of eContracts may be deleted and purged by Vendor without prior notice after the period available for transition services has expired pursuant to the terms described in Section 30)b). Agency may, at its option and wholly at Agency's risk, direct that any eContract be deleted or purged at a time stated by Agency and prior to the end of the Term.

ii) Uncompleted eContracts. Vendor may at its sole discretion delete an uncompleted eContract from the System immediately and without notice upon earlier of: a) expiration of the Envelope (where Agency has established an expiration for such Envelope, not to exceed 365 days); or b) expiration of the Order Term.

iii) Notwithstanding anything to the contrary in this Contract or any subsequent agreement between the parties, Transaction Data associated with deleted eContracts will be retained by Vendor permanently, and will be maintained per the confidentiality obligations of this Contract.

k) Each Vendor Envelope Allowance or Seat Subscription purchased by an Agency shall include the right to and access to any upgrades, updates, maintenance, releases or other enhancements or modifications made generally available to Vendor's customers of the Software Applications and Services provided herein without the Vendor requiring a separate maintenance or support agreement. The Agency may use the Software Applications with any computer, computer system, server, or desktop workstation owned or utilized by the Agency or its constituent educational institutions that meet the Authorized User Minimum System and Software Requirement defined in the Specifications. User access to the Software Applications shall be through User identification and security procedures. The Agency agrees to use its best efforts to see that its employees and users of all Software Application rights provided hereunder comply with the terms and conditions set forth in this Agreement, and any Exhibits or Amendments hereto. The Agency shall notify the Vendor of any material unauthorized use of any password or account, or any other known or suspected breach of security access. The Agency also agrees to refrain from taking any steps, such as reverse engineering, reverse assembly or reverse compilation to derive a source code equivalent to the Software Applications or any portion thereof. No license is granted to use the Software Applications to perform services for commercial third parties (so-called "service bureau" uses). If the Software Application fees are based upon the number of Users and hosted instances, the number of Users/hosted instances available may be increased at any time, subject to the restrictions on the maximum number of Users specified in the Furnish and Deliver Table herein (above) except by mutual agreement and State Procurement approval.

l) The State's subscription to use the Software Application and its associated services neither transfers, vests, nor infers any title or other ownership right in any intellectual property rights of the Vendor or any third party, nor does this license transfer, vest, or infer any title or other ownership right in any source code associated with the Software Application unless otherwise agreed to by the Parties. The subscription will not be construed as a sale of any ownership rights in the Software Application unless Custom Software is developed as a Work for Hire pursuant to other agreement(s). Any Software Applications or technical and business information owned by Vendor or its suppliers or licensors made accessible or furnished to the State shall be and remain the property of the Vendor or other party, respectively.

m) The Software shall be in good working order; determined as operating in conformance with Vendor's standard Specifications. The State shall notify the Vendor if the Software is not in good working order or inaccessible during the term of the Contract. Vendor shall, at its option, either repair or replace any Software reported as not in good working order during the applicable contract term without cost to the State. Vendor shall support the Software pursuant to its Service and Support Level Commitment ("SLA"). The Software Applications shall be provided and the State Data accessible by the State's users at a rate of 99.99%, 24 x 7, with the exception of scheduled outages for maintenance, all as specified hereinabove and further detailed in Vendor's Service and Support Level Commitment ("SLA").

n) Support. Vendor shall provide the State and its users with telephone access to technical support engineers for assistance in the proper installation and use of the Software, and to report and resolve Software problems, during normal business hours, 7:00 AM - 7:00 PM Eastern Time, Monday-Friday. Vendor shall respond to the telephone requests for Program maintenance service, and respond to critical incidents and non-critical incidents pursuant to Vendor's SLA, for calls made at any time. Vendor warrants that its support and customer service and assistance will be performed in accordance with generally accepted industry standards.

- i) Critical Incident
- ii) Non-Critical Incident

o) Security. Vendor shall use all commercially reasonable efforts to provide a secure environment for the State to utilize the Web-Based Software Applications and the associated services.

p) Vendor shall provide all encryption or identification codes or authorizations that are necessary or proper for the operation of the licensed Software.

7) Maintenance/Support Services: Vendor agrees to provide the following services for the current version and one previous version of any Software provided with the Deliverables, commencing upon installation of the Deliverables or delivery of the Software:

a) Error Correction. Upon notice by State of a problem with the Software (which problem can be verified), Vendor shall use reasonable efforts to correct or provide a working solution for the problem. The State shall comply with all reasonable instructions or requests of Vendor in attempts to correct an error or defect in the Program. Vendor and the State shall act promptly and in a reasonably timely manner in communicating error or problem logs, other related information, proposed solutions or workarounds, and any action as may be necessary or proper to obtain or affect maintenance services under this Paragraph.

b) Vendor shall notify the State of any material errors or defects in the Deliverables known, or made known to Vendor from any source during the Contract term that could cause the production of inaccurate or otherwise materially incorrect, results. Vendor shall initiate actions as may be commercially necessary or proper to effect corrections of any such errors or defects.

c) Updates. Vendor shall provide to the State, at no additional charge, all new releases and bug fixes (collectively referred to as "Changes") for any Software Deliverable developed or published by Vendor and made generally available to its other customers at no additional charge. All such Updates shall be a part of the Program and Documentation and, as such, be governed by the provisions of this Contract.

d) Telephone Assistance. Vendor shall provide the State with telephone access to technical support engineers for assistance in the proper installation and use of the Software, and to report and resolve Software problems, during normal business hours, 7:00 AM - 7:00 PM Eastern Time, Monday-Friday. Vendor shall respond to the telephone requests for Program maintenance service, within four hours, for calls made at any time.

8) Travel Expenses: Vendor may be reimbursed for travel expenses arising under the performance of this Contract at the out-of-state rates set forth in GS §138-6; as amended from time to time. Vendor agrees to use the lowest available airfare not requiring a weekend stay and to use the lowest available rate for rental vehicles. All Vendor incurred travel expenses shall be billed on a monthly basis, shall be supported by receipt and shall be paid by the State within thirty (30) days after invoice approval. Travel expenses exceeding the

foregoing rates shall not be paid by the State. The State will reimburse travel allowances only for days on which the Vendor is required to be in North Carolina performing services under this Contract.

9) Governmental Restrictions: In the event any restrictions are imposed by governmental requirements that necessitate alteration of the material, quality, workmanship, or performance of the Deliverables offered prior to delivery thereof, the Vendor shall provide written notification of the necessary alteration(s) to the Agency Contract Administrator. The State reserves the right to accept any such alterations, including any price adjustments occasioned thereby, or to cancel the Contract. The State may advise Vendor of any restrictions or changes in specifications required by North Carolina legislation, rule or regulatory authority that require compliance by the State. In such event, Vendor shall use its best efforts to comply with the required restrictions or changes. If compliance cannot be achieved by the date specified by the State, the State may terminate this Contract and compensate Vendor for sums due under the Contract.

a) Where any change in Law or Regulatory Requirements impacting the Deliverables or Services to be delivered under the Contract, the State shall pay additional, previously agreed amounts to compensate Vendor for any additional reasonable expenses that Vendor may incur in making and sustaining the required changes to the Services or Deliverables amounts as the Parties may mutually agree; provided, however if such change in Law or Regulatory Requirements affects other Vendor customers then receiving substantially similar Services or Deliverables, then Vendor will use reasonable efforts to allocate that cost of changes or modifications to such Services and Deliverables and performance of such Services and Deliverables across its affected customers and the State will pay only its pro rata share associated with such changes or modifications. Upon the State's request the Vendor shall provide documentation to substantiate the Vendor's allocation of such cost(s). As an alternative to agreeing to pay additional amounts as set forth above, the State shall have the right to cancel those portions of the Contract to which the additional expenses pertain.

10) Prohibition Against Contingent Fees and Gratuities: Vendor warrants that it has not paid, and agrees not to pay, any bonus, commission, fee, or gratuity to any employee or official of the State for the purpose of obtaining any contract or award issued by the State. Vendor further warrants that no commission or other payment has been or will be received from or paid to any third party contingent on the award of any contract by the State, except as shall have been expressly communicated to the State Purchasing Agent in writing prior to acceptance of the Contract or award in question. Each individual signing below warrants that he or she is duly authorized by their respective Party to sign this Contract and bind the Party to the terms and conditions of this Contract. Vendor and their authorized signatory further warrant that no officer or employee of the State has any direct or indirect financial or personal beneficial interest, in the subject matter of this Contract; obligation or contract for future award of compensation as an inducement or consideration for making this Contract. Subsequent discovery by the State of non-compliance with these provisions shall constitute sufficient cause for immediate termination of all outstanding contracts. Violations of this provision may result in debarment of the Vendor(s) as permitted by 9 NCAC 06B.1030, or other provision of law.

11) Availability of Funds: Any and all payments to Vendor are expressly contingent upon and subject to the appropriation, allocation and availability of funds to the Agency for the purposes set forth in this Contract. If this Contract or any Purchase Order issued hereunder is funded in whole or in part by federal funds, the Agency's performance and payment shall be subject to and contingent upon the continuing availability of said federal funds for the purposes of the Contract or Purchase Order. If the term of this Contract extends into fiscal years, subsequent to that in which it is approved, such continuation of the Contract is expressly contingent upon the appropriation, allocation and availability of funds by the N.C. Legislature for the purposes set forth in the Contract. If funds to effect payment are not available, the Agency will provide written notification to Vendor. If the Contract is terminated under this paragraph, Vendor agrees to take back any affected Deliverables and software not yet delivered under this Contract, terminate any services supplied to the Agency under this Contract, and relieve the Agency of any further obligation thereof. The State shall remit payment for Deliverables and services accepted prior to the date of the aforesaid notice in conformance with the payment terms.

12) Compliance with Laws: The Vendor shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business, including those of federal, state, and local agencies having jurisdiction and/or authority.

a) Vendor will obtain and maintain all governmental approvals (as defined below) applicable to Vendor in the conduct of its business and will identify, interpret and comply in all material respects with all laws, (including those under common law) statutes, codes, rules, regulations, reporting or licensing requirements, ordinances, and other pronouncement having the effect of law of the United States or any state, county, city, or other political subdivision, including those promulgated, interpreted or enforced by any government or regulatory authority, presently or hereinafter in effect ("Laws") applicable to Vendor for the provision, receipt and use of the Services, and the consummation of the transactions contemplated by the Contract (the "Regulatory Requirements"). Regulatory Requirements include all Laws concerning fair employment and employment of the disabled and concerning the treatment of all employees without regard to discrimination by reason of race, color, religion, sex, national origin, or physical disability. Regulatory Requirements also include any guidance, bulletins, white papers, pronouncements, reports or similar communications issued by any Governmental Authority or applicable self-regulatory or industry body, whether or not such items or materials have the force of Law, to the extent determined by the State in its discretion.

b) In addition, as part of the Services being provided by Vendor, Vendor will, and will cause its employees, agents and subcontractors to provide, notwithstanding anything to the contrary set forth in the Contract and subject to 33) (Changes), all assistance reasonably related to the Services provided by Vendor necessary to enable the State to comply with the Regulatory Requirements.

c) In providing Services to the State, and without limiting or modifying in any respect the Vendor's obligations, Vendor shall comply, and shall cause each of its employees and subcontractors to comply at all times, with State policies that are of general application to State contractors or that Vendor has otherwise agreed to comply with, including, without limitation, the Statewide Information Technology Security Manual and the Agency's Security Policies and Standards.

d) Subject to 33) (Changes), where any change in Law or Regulatory Requirements impacting the Services, (* insert Agency specific requirements, Project name, etc.) requires a substantial change in the Services or Deliverables to be delivered under this Contract, the State shall pay such amounts as the Parties may agree; provided, however if such change in Law or Regulatory Requirements affects other Vendor customers, then Vendor will use reasonable efforts to allocate that cost of modifications to its Deliverables and performance of services across its affected customers and the State will pay only its pro rata share associated with such modifications. Upon the State's request the Vendor shall provide documentation to substantiate the Vendor's allocation of such cost. As an alternative to agreeing to pay additional amounts as set forth above, the State shall have the right to cancel those portions of the Contract to which the additional expenses pertain.

e) The Vendor shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business, including those of federal, state, and local agencies having jurisdiction and/or authority.

13) Payment Terms: Payment terms are Net 30 days after receipt of correct invoice for the subscription fees for use of the Software, or for Professional Services, or acceptance of the Deliverables, whichever is later; unless a period of more than thirty (30) days is required by the Agency. The Purchasing State Agency is responsible for all payments under the Contract. No additional charges to the Agency will be permitted based upon, or arising from, the Agency's use of a Business Procurement Card. The State may exercise any and all rights of Set Off as permitted in Chapter 105A-1 et seq. of the N.C. General Statutes and applicable Administrative Rules. Upon Vendor's written request of not less than 30 days and approval by the State or Agency, the Agency may:

a) Forward the Vendor's payment check(s) directly to any person or entity designated by the Vendor, or

b) Include any person or entity designated in writing by Vendor as a joint payee on the Vendor's payment check(s), however

c) In no event shall such approval and action obligate the State to anyone other than the Vendor and the Vendor shall remain responsible for fulfillment of all Contract obligations.

d) An undisputed invoice shall be limited to the following: an undisputed invoice is an invoice for which the State and/or the Purchasing Agency has not disputed the invoice in writing sent to the Vendor on the grounds of an invoice error within thirty (30) days from the invoice date. That is, in order for the State or the applicable Purchasing Agency to dispute any invoice under this Agreement, such dispute must be made in writing to Vendor within thirty (30) days of the invoice date. Upon Vendor's receipt of such disputed invoice notice, Vendor will work to correct the applicable invoice error, provided that such dispute notice shall not relieve the State or the applicable Purchasing Entity from its payment obligations for the undisputed items on the invoice or for any disputed items that are ultimately corrected. The Purchasing Agency is not required to pay the Vendor for any goods and/or services provided without a written purchase order from the appropriate Purchasing Agency. In addition, all goods and/or services provided must meet all terms, conditions, and specifications of the Contract and purchase order and be accepted as satisfactory by the Purchasing Agency before payment will be issued.

14) Acceptance Criteria: In the event acceptance of Deliverables is not described in additional Contract documents, the State shall have the obligation to notify Vendor, in writing ten calendar days following installation of any Deliverable described in the Contract if it is not acceptable. The notice shall specify in reasonable detail the reason(s) a deliverable is unacceptable. Acceptance by the State shall not be unreasonably withheld; but may be conditioned or delayed as required for installation and/or testing of Deliverables. Final acceptance is expressly conditioned upon completion of all applicable inspection and testing procedures. Should the Deliverables fail to meet any specifications or acceptance criteria the State may exercise any and all rights hereunder, including such rights provided by the Uniform Commercial Code as adopted in North Carolina. Deliverables discovered to be defective or failing to conform to the specifications may be rejected upon initial inspection or at any later time if the defects contained in the Deliverables or non-compliance with the specifications was not reasonably ascertainable upon initial inspection. If the Vendor fails to promptly cure the defect or replace the Deliverables, the State reserves the right to cancel the Purchase Order, contract with a different Vendor, and to invoice the original Vendor for any differential in price over the original Contract price. When Deliverables are rejected, the Vendor must remove the rejected Deliverables from the premises of the State Agency within seven (7) calendar days of notification, unless otherwise agreed by the State Agency. Rejected items may be regarded as abandoned if not removed by Vendor as provided herein.

15) Equal Employment Opportunity: Vendor shall comply with all Federal and State requirements concerning fair employment and employment of the disabled, and concerning the treatment of all employees without regard to discrimination by reason of race, color, religion, sex, national origin or physical disability.

16) Inspection at Vendor's Site: The State reserves the right to inspect, during Vendor's regular business hours at a reasonable time, upon notice of not less than two (2) weeks, and at its own expense, the prospective Deliverables comprising equipment or other tangible goods, or the plant or other physical facilities of a prospective Vendor prior to Contract award, and during the Contract term as necessary or proper to ensure conformance with the specifications/requirements and their adequacy and suitability for the proper and effective performance of the Contract.

17) Advertising/Press Release: The Vendor absolutely shall not publicly disseminate any information concerning the Contract without prior written approval from the State or its Agent. For the purpose of this provision of the Contract, the Agent is the Purchasing Agency Contract Administrator unless otherwise named in the solicitation documents.

18) Confidentiality: In accordance with 9 NCAC 06B.0103, 06B.0207 and 06B.1001 and to promote maximum competition in the State competitive bidding process, the State may maintain the confidentiality of certain types of information described in N.C. Gen. Stat. §132-1 et. seq. Such information may include trade

secrets defined by N.C. Gen. Stat. §66-152 and other information exempted from the Public Records Act pursuant to N.C. Gen. Stat. §132-1.2. Vendor may designate appropriate portions of its response as confidential, consistent with and to the extent permitted under the Statutes and Rules set forth above, by marking the top and bottom of pages containing confidential information with a legend in boldface type "CONFIDENTIAL". By so marking any page, the Vendor warrants that it has formed a good faith opinion, having received such necessary or proper review by counsel and other knowledgeable advisors that the portions marked confidential meet the requirements of the Rules and Statutes set forth above. **However, under no circumstances shall price information be designated as confidential.** The State may serve as custodian of Vendor's confidential information and not as an arbiter of claims against Vendor's assertion of confidentiality. If an action is brought pursuant to N.C. Gen. Stat. §132-9 to compel the State to disclose information marked confidential, the Vendor agrees that it will intervene in the action through its counsel and participate in defending the State, including any public official(s) or public employee(s). The Vendor agrees that it shall hold the State and any official(s) and individual(s) harmless from any and all damages, costs, and attorneys' fees awarded against the State in the action. The State agrees to promptly notify the Vendor in writing of any action seeking to compel the disclosure of Vendor's confidential information. The State shall have the right, at its option and expense, to participate in the defense of the action through its counsel. The State shall have no liability to Vendor with respect to the disclosure of Vendor's confidential information ordered by a court of competent jurisdiction pursuant to N.C. Gen. Stat. §132-9 or other applicable law.

a) Care of Information: Vendor agrees to use commercial best efforts to safeguard and protect any data, documents, files, and other materials received from the State or the Agency during performance of any contractual obligation from loss, destruction or erasure.

b) Vendor warrants that all its employees and any third party Vendors or subcontractors are subject to a non-disclosure and confidentiality agreement enforceable in North Carolina. Vendor will, upon request of the State, verify and produce true copies of any such agreements. Production of such agreements by Vendor may be made subject to applicable confidentiality, non-disclosure or privacy laws; provided that Vendor produces satisfactory evidence supporting exclusion of such agreements from disclosure under the N.C. Public Records laws in NCGS §132-1 et seq. The State may, in its sole discretion, provide a non-disclosure and confidentiality agreement satisfactory to the State for Vendor's execution. The State may exercise its rights under this subparagraph as necessary or proper, in its discretion, to comply with applicable security regulations or statutes including, but not limited to 26 USC 6103 and IRS Publication 1075, (Tax Information Security Guidelines for Federal, State, and Local Agencies), HIPAA, 42 USC 1320(d) (Health Insurance Portability and Accountability Act), any implementing regulations in the Code of Federal Regulations, and any future regulations imposed upon the Office of Information Technology Services or the N.C. Department of Revenue pursuant to future statutory or regulatory requirements.

c) Nondisclosure: Vendor agrees and specifically warrants that it, its officers, directors, principals and employees, and any subcontractors, shall hold all information received during performance of this Contract in the strictest confidence and shall not disclose the same to any third party without the express written approval of the State.

19) Deliverables: Deliverables, as used herein, shall comprise all project materials, including goods, software licenses, data, and documentation created during the performance or provision of Professional Services hereunder. Deliverables are the property of the State of North Carolina. Proprietary Vendor materials licensed to the State shall be identified to the State by Vendor prior to use or provision of services hereunder and shall remain the property of the Vendor. Embedded software or firmware shall not be a severable Deliverable. Deliverables include "Work Product" and means any expression of Licensor's findings, analyses, conclusions, opinions, recommendations, ideas, techniques, know-how, designs, programs, enhancements, and other technical information; but not source and object code or software. All Software source and object code is the property of Licensor.

20) Late Delivery, Back Order: Vendor shall advise the Agency contact person or office immediately upon determining that any Deliverable will not, or may not, be delivered at the time or place specified. Together with such notice, Vendor shall state the projected delivery time and date. In the event the delay projected by

Vendor is unsatisfactory, the Agency shall so advise Vendor and may proceed to procure substitute Deliverables or services.

21) Patent, Copyright, and Trade Secret Protection:

- a) Vendor has created, acquired or otherwise has rights in, and may, in connection with the performance of services for the State, employ, provide, create, acquire or otherwise obtain rights in various concepts, ideas, methods, methodologies, procedures, processes, know-how, techniques, models, templates and general purpose consulting and software tools, utilities and routines (collectively, the "Vendor Technology"). To the extent that any Vendor Technology is contained in any of the Deliverables including any derivative works, the Vendor hereby grants the State a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to use such Vendor Technology in connection with the Deliverables for the State's purposes.
- b) Vendor shall not acquire any right, title and interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data or derivative works thereof, or other work products provided by the State to Vendor. The State hereby grants Vendor a royalty-free, fully paid, worldwide, perpetual, non-exclusive license for Vendor's internal use to non-confidential Deliverables first originated and prepared by the Vendor for delivery to the State.
- c) The Vendor, at its own expense, shall defend any action brought against the State to the extent that such action is based upon a third party claim that the services or Deliverables supplied by the Vendor, or the operation of such Deliverables pursuant to a current version of Vendor-supplied software, infringes a patent, or copyright or violates a trade secret in the United States. The Vendor shall pay those costs and damages finally awarded against the State in any such action. Such defense and payment shall be conditioned on the following:
 - i) That the Vendor shall be notified within a reasonable time in writing by the State of any such claim; and,
 - ii) That the Vendor shall have the sole control of the defense of any action on such claim and all negotiations for its settlement or compromise provided, however, that the State shall have the option to participate in such action at its own expense.
- d) Should any services or software supplied by Vendor, or the operation thereof become, or in the Vendor's opinion are likely to become, the subject of a third party claim of infringement of a patent, copyright, or a trade secret in the United States, the State shall permit the Vendor, at its option and expense, either to procure for the State the right to continue using the goods/hardware or software, or to replace or modify the same to become non infringing and continue to meet procurement specifications in all material respects. If neither of these options can reasonably be taken, or if the use of such goods/hardware or software by the State shall be prevented by injunction, the Vendor agrees to take back such goods/hardware or software, and refund any sums the State has paid Vendor less any reasonable amount for use or damage and make every reasonable effort to assist the State in procuring substitute Deliverables. If, in the sole opinion of the State, the return of such infringing Deliverables makes the retention of other items of Deliverables acquired from the Vendor under this Contract impractical, the State shall then have the option of terminating the Contract, or applicable portions thereof, without penalty or termination charge. The Vendor agrees to take back such Deliverables and refund any sums the State has paid Vendor less any reasonable amount for use or damage.
- e) Vendor will not be required to defend or indemnify the State if any claim by a third party against the State for infringement or misappropriation (i) results from the State's alteration of any Vendor-branded product or Deliverable, or (ii) results from the continued use of the good(s) or Services and Deliverables after receiving notice they infringe a trade secret of a third party.
- f) Nothing stated herein, however, shall affect Vendor's ownership in or rights to its preexisting intellectual property and proprietary rights.

22) Access to Persons and Records: Pursuant to N.C. General Statute 147-64.7, the Agency, the State Auditor, appropriate federal officials, and their respective authorized employees or agents are authorized to

examine all books, records, and accounts of the Vendor insofar as they relate to transactions with any department, board, officer, commission, institution, or other Agency of the State of North Carolina pursuant to the performance of this Contract or to costs charged to this Contract. The Vendor shall retain any such books, records, and accounts for a minimum of three (3) years after the completion of this Contract. Additional audit or reporting requirements may be required by any Agency, if in the Agency's opinion, such requirement is imposed by federal or state law or regulation.

23) Assignment: Vendor may not assign this Contract or its obligations hereunder except as permitted by 09 NCAC 06B.1003 and this Paragraph. Vendor shall provide reasonable notice of not less than thirty (30) days prior to any consolidation, acquisition, or merger. Any assignee shall affirm this Contract attorning to the terms and conditions agreed, and that Vendor shall affirm that the assignee is fully capable of performing all obligations of Vendor under this Contract. An assignment may be made, if at all, in writing by the Vendor, Assignee and the State setting forth the foregoing obligation of Vendor and Assignee.

24) Insurance Coverage: During the term of the Contract, the Vendor at its sole cost and expense shall provide commercial insurance of such type and with such terms and limits as may be reasonably associated with the Contract. As a minimum, the Vendor shall provide and maintain the following coverage and limits:

a) **Worker's Compensation** - The Vendor shall provide and maintain Worker's Compensation Insurance, as required by the laws of North Carolina, as well as employer's liability coverage with minimum limits of \$100,000.00, covering all of Vendor's employees who are engaged in any work under the Contract. If any work is sublet, the Vendor shall require the subcontractor to provide the same coverage for any of his employees engaged in any work under the Contract; and

b) **Commercial General Liability** - General Liability Coverage on a Comprehensive Broad Form on an occurrence basis in the minimum amount of \$2,000,000.00 Combined Single Limit (Defense cost shall be in excess of the limit of liability); and

c) **Automobile** - Automobile Liability Insurance, to include liability coverage, covering all owned, hired and non-owned vehicles, used in connection with the Contract. The minimum combined single limit shall be \$500,000.00 bodily injury and property damage; \$500,000.00 uninsured/under insured motorist; and \$5,000.00 medical payment; and

d) Providing and maintaining adequate insurance coverage described herein is a material obligation of the Vendor and is of the essence of this Contract. All such insurance shall meet all laws of the State of North Carolina. Such insurance coverage shall be obtained from companies that are authorized to provide such coverage and that are authorized by the Commissioner of Insurance to do business in North Carolina. The Vendor shall at all times comply with the terms of such insurance policies, and all requirements of the insurer under any such insurance policies, except as they may conflict with existing North Carolina laws or this Contract. The limits of coverage under each insurance policy maintained by the Vendor shall not be interpreted as limiting the Vendor's liability and obligations under the Contract.

25) Dispute Resolution: The parties agree that it is in their mutual interest to resolve disputes informally. A claim by the Vendor shall be submitted in writing to the Agency Contract Administrator for decision. A claim by the State shall be submitted in writing to the Vendor's Contract Administrator for decision. The Parties shall negotiate in good faith and use all reasonable efforts to resolve such dispute(s). During the time the Parties are attempting to resolve any dispute, each shall proceed diligently to perform their respective duties and responsibilities under this Contract. If a dispute cannot be resolved between the Parties within thirty (30) days after delivery of notice, either Party may elect to exercise any other remedies available under this Contract, or at law. This term shall not constitute an agreement by either party to mediate or arbitrate any dispute.

26) Default: In the event any Deliverable furnished by the Vendor during performance of any Contract term fails to conform to any material requirement of the Contract specifications, notice of the failure is provided by the State and if the failure is not cured within ten (10) days, or Vendor fails to meet the requirements of Paragraph 14) (Acceptance) herein, the State may cancel and procure the articles or services from other sources; holding Vendor liable for any excess costs occasioned thereby, subject only to the limitations provided in Paragraphs 30) (Limitation of Liability) and 31) (Liability for Injury to Persons or Damage to

Property) and the obligation to informally resolve disputes as provided in Paragraph 25) (Dispute Resolution) of these Terms and Conditions. Default may be cause for debarment as provided in 09 NCAC 06B.1030. The State reserves the right to require performance guaranties pursuant to 09 NCAC 06B.1031 from the Vendor without expense to the State. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.

- a) If Vendor fails to deliver Deliverables within the time required by this Contract, the State may provide written notice of said failure to Vendor, and by such notice require payment of a penalty.
- b) Should the State fail to perform any of its obligations upon which Vendor's performance is conditioned, Vendor shall not be in default for any delay, cost increase or other consequences due to the State's failure. Vendor will use reasonable efforts to mitigate delays, costs or expenses arising from assumptions in the Vendor's bid documents that prove erroneous or are otherwise invalid. Any deadline that is affected by any such failure in assumptions or performance by the State shall be extended by an amount of time reasonably necessary to compensate for the effect of such failure.
- c) Vendor shall provide a plan to cure any default if requested by the State. The plan shall state the nature of the default, the time required for cure, any mitigating factors causing or tending to cause the default, and such other information as the Vendor may deem necessary or proper to provide.

27) Waiver of Default: Waiver by either party of any default or breach by the other Party shall not be deemed a waiver of any subsequent default or breach and shall not be construed to be a modification or novation of the terms of this Contract, unless so stated in writing and signed by authorized representatives of the Agency and the Vendor, and made as an amendment to this Contract pursuant to Paragraph 40) herein below.

28) Termination: Any notice or termination made under this Contract shall be transmitted via US Mail, Certified Return Receipt Requested. The period of notice for termination shall begin on the day the return receipt is signed and dated.

- a) The parties may mutually terminate this Contract by written agreement at any time.
- b) The State may terminate this Contract, in whole or in part, pursuant to Paragraph 26) (Default), or pursuant to the Special Terms and Conditions in the Solicitation Documents, if any, or for any of the following:
 - i) Termination for Cause: In the event any goods, software, or service furnished by the Vendor during performance of any Contract term fails to conform to any material requirement of the Contract, and the failure is not cured within the specified time after providing written notice thereof to Vendor, the State may cancel and procure the articles or services from other sources; holding Vendor liable for any excess costs occasioned thereby, subject only to the limitations provided in Paragraphs 30) (Limitation of Liability) and 31) (Liability for Injury to Persons or Damage to Property) herein. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract. Vendor shall not be relieved of liability to the State for damages sustained by the State arising from Vendor's breach of this Contract; and the State may, in its discretion, withhold any payment due as a set off until such time as the damages are finally determined or as agreed by the parties. Voluntary or involuntary Bankruptcy or receivership by Vendor shall be cause for termination.
 - ii) Termination For Convenience Without Cause: The State may terminate service and indefinite quantity contracts, in whole or in part by giving thirty (30) days prior notice in writing to the Vendor. Vendor shall be entitled to sums due as compensation for Deliverables provided and Services (whether Subscription or Professional Services) performed in conformance with the Contract. In the event the Contract is terminated for the convenience of the State, the Agency will pay for all Deliverables provided and Professional Services performed in conformance with the Contract up to the date of termination. In the event the Contract is terminated for the convenience of the State, the Agency will not be entitled to a refund of any prepaid fees for the Subscription Services, and the Agency shall not be relieved of its payment obligations for the Subscription Services covered by any Purchase Order for the remainder of the term committed to in such Purchase Order.

iii) Termination for Change in Control. In the event of a Change in Control of Vendor, (a) Vendor will promptly provide notice to the State of such event, and (b) the State has the right, but not the obligation, within thirty (30) days of receipt of such notice, to terminate the Agreement by giving Vendor notice of termination at least thirty (30) days prior to the termination date specified in the notice. "Change in Control" means the transfer of the control of Vendor from the person(s), entity or entities who hold such control on the Effective Date of the Agreement to one or more other persons or entities. "Control" means the ability to direct the voting of more than fifty percent (50%) of the stock or shares (or other equity interests of Vendor) entitled to vote for the election of the board of directors or other governing body of Vendor.

iv) Termination for Financial Instability. The State may terminate this Agreement by providing written notice to such effect (a) in the event that the State determines in its sole but reasonable discretion that Vendor has become financially unstable to the point of threatening the ability of Vendor to perform its obligations under this Agreement, (b) upon Vendor's institution of insolvency, receivership or bankruptcy proceedings or any other proceedings for the settlement of its debts, (c) upon the institution of such proceedings against Vendor, which are not dismissed or otherwise resolved in Vendor's favor within sixty (60) days thereafter, (d) upon Vendor's making a general assignment for the benefit of creditors, or (e) upon Vendor's dissolution or ceasing to conduct business in the normal course. Such termination shall be effective at the close of business on the date specified in the written notice. In the event that State elects to terminate the Agreement pursuant to this Section, Vendor shall be notified in writing by the means set forth in the Agreement for providing notice, specifying the date of termination. In the event of the filing of a petition in bankruptcy by or against Vendor or any subcontractor, Vendor shall promptly advise the State of such action.

c) Procedures on Termination or Expiration: Upon termination or expiration of the Agreement, (i) Vendor shall, on the date specified in the notice of termination or on the date of expiration, cease performing any Services or Hosting Services; return, or make provision to return, State data to the State Agency in accordance with the Transition Services described below in 29)b) or otherwise delete all Customer Content from Vendor's computer systems, excepting Transaction Data, and shall ensure any storage media if not reusable is disposed of in an appropriate and secure manner; and (ii) Customer shall cease use of the System.

29) Transition Upon Termination Or Expiration:

a) Agency may provide notice of its intent to transition the Solution upon termination or expiration of the Agreement. If Agency terminates the Agreement, Agency shall pay Vendor those undisputed sums to which it is entitled, as well as payment for third party licenses.

b) Vendor agrees that, following notice of termination or expiration of the Agreement for a period of twelve (12) months and upon Agency's election, it shall use reasonable efforts and cooperate with Agency or third parties working on behalf of Agency to provide for an orderly transition of the completed Envelopes. At Agency's request, Vendor shall provide the staff services and assistance reasonably required for such orderly transition as well as a variety of options for continuing service and/or transitioning services and assets, provided that Agency shall pay all reasonable costs and expenses which Vendor actually incurs in connection with such orderly transfer, provided further that hourly rates for professional services rendered during the transition shall not exceed the hourly rates specified in Section V of the Agreement.

c) If the Agency elects to secure Vendor's services during a period of transition services, Vendor and Agency will work together to develop and implement a Transition Plan, which will define the overall tasks, schedules, deliverables, and resource requirements for the transition services period. The completed Transition Plan, if accepted by Agency, shall be prepared as a Statement of Work and executed by the Parties. Vendor shall be allowed to use, at no charge, the Agency facilities then being used to perform the Agreement for the purposes of providing transition assistance.

d) The parties anticipate that the Vendor and Agency will develop a Transition Plan, and consider the following items as potential elements:

- i) Responsibilities by resource for operational support during the transition services period.
 - ii) Identification of any Deliverables that have not been delivered, that have been delivered but not accepted, or that have been rejected and a proposed resolution for all such identified Deliverables.
 - iii) A list of detailed documentation about the technical infrastructure and applications to be provided during the transition services period to support ongoing support and maintenance of Solution, and provision for delivery of all documentation, configurations, design assumptions, manuals, business logic and other such informational records necessary for continued operation of the Solution.
 - iv) A work plan for each stage of the transition services.
 - v) Plans for coordination and transition of specific responsibilities from Vendor to Agency. This must address vendor management with single sourced accountability.
 - vi) Help Desk Operations.
 - vii) A list of operational statistics to be provided during the transition services period, including resource consumption, system performance, and application activity in both aggregated and trended forms.
 - viii) An inventory of third party products for which the licenses will be transferred from Vendor to the Agency. This inventory shall be delivered together with full executed copies of all license agreements and assignments therefore acceptable to the State.
 - ix) Any work in process or to be performed under any Work Order in operation at the time Agency requests transition.
 - x) Return of Agency Data & Other Property; and destruction and verification for confidential records, software, scripts.
- e) In addition, the parties anticipate that the Transition Plan will, at a minimum, specifically provide for transition of the following functions to Agency:
- i) Training Support - Knowledge and Process Transition.
 - ii) Project Management Support: Knowledge and Process Transition, Management Tool Transition.
 - iii) Help Desk Operations: Knowledge and Process Transition Training, Tool Transition.
 - iv) Operations Transition: Technical Operations, Knowledge and Process Transitions.
 - v) Training
 - vi) Production Hardware Infrastructure Transition: Server Based systems, Network Based systems, Database systems, Web Based systems, Data Migration.
 - vii) Development Environment Hardware Infrastructure Transition: Server Based systems, Network Based systems, Database systems, Web Based systems.
 - viii) Data Migration
 - ix) Hardware Infrastructure Test Plan
 - x) Software Infrastructure Transition: Licensing, Dependencies, Third-Party Software and Tools, Testing Plan, Level of Certification, Operations Transition.
 - xi) Network Connectivity Migration Planning: Training, Knowledge and Process Transitions, Front-End Connectivity, Back-End Connectivity.
 - xii) Environmental: Cabling Environment, Mounting System Rack, Enterprise Systems and High Availability.

- xiii) Application Operations: Knowledge and Process Transition, Application Component Transition, Vendor Proprietary Software Transition License Transition.
- xiv) Operations Transitions

30) Limitation of Vendor's Liability:

- a) Where Deliverables are under the State's exclusive management and control, the Vendor shall not be liable for direct damages caused by the State's failure to fulfill any State responsibilities of assuring the proper use, management and supervision of the Deliverables and programs, audit controls, operating methods, office procedures, or for establishing all proper checkpoints necessary for the State's intended use of the Deliverables.
- b) The Vendor's liability for damages to the State for any cause whatsoever, and regardless of the form of action, whether in contract or in tort, shall be limited to two times the value of the Contract.
- c) The foregoing limitation of liability shall not apply to the payment of costs and damage awards referred to in the Paragraph entitled "Patent, Copyright, and Trade Secret Protection", to third party claims covered by other specific provisions calling for liquidated damages or specifying a different limit of liability, or to third party claims for injury to persons or damage to property caused by Vendor's negligence or willful or wanton conduct. This limitation of liability does not apply to the receipt of court costs or attorney's fees that might be awarded by a court in addition to damages after litigation based on this Contract.
- d) Limitation of Liability for Software Services or Deliverables:
 - i) Where Deliverables are under the State's exclusive management and control, Vendor shall not be liable for any damages caused by the State's failure to fulfill any State responsibilities including, without limitation, those relating to assuring the proper use, management and supervision of the equipment and programs, audit controls, operating methods, office procedures or for establishing all property checkpoints necessary for the State's intended use of the Deliverables.
 - ii) The Vendor's liability for damages to the State for any cause whatsoever, and regardless of the form of action, whether in contract or in tort, shall not exceed two times the value of the contract, but in no event shall the liability for damages be less than the total value of the contract.
 - iii) WITH THE EXCEPTIONS OF INTELLECTUAL PROPERTY RIGHTS INFRINGEMENT ACTIONS, THE STATE'S CONSTITUTIONAL RIGHTS AS A SOVEREIGN, AND PENALTIES IMPOSED UPON THE STATE BY ANY FEDERAL ENTITY OR EXPENDITURES OF PUBLIC FUNDS REQUIRED OR RESULTING FROM AN OPERATIONAL FAILURE OF THE DELIVERABLE(S) OR SERVICES PROVIDED HEREUNDER, BUT NOTWITHSTANDING ANY OTHER TERM TO THE CONTRARY CONTAINED IN THIS CONTRACT, NEITHER PARTY NOR THEIR RESPECTIVE AFFILIATES SHALL, UNDER ANY CIRCUMSTANCES, BE LIABLE TO THE OTHER PARTY OR ITS AFFILIATES (I) FOR ANY CLAIM BASED UPON ANY THIRD PARTY CLAIM, (II) FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES OF ANY NATURE WHATSOEVER, INCLUDING, WITHOUT LIMITATION, LOST PROFITS, LOST SAVINGS OR OTHER ECONOMIC CONSEQUENTIAL DAMAGES, WHETHER RESULTING FROM DELAYS, LOSS OF DATA, INTERRUPTION OF SERVICE OR OTHERWISE, EVEN IF A PARTY OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR (III) FOR ANY PUNITIVE OR EXEMPLARY DAMAGES OF ANY NATURE WHATSOEVER.

31) Vendor's Liability for Injury to Persons or Damage to Property:

- a) The Vendor shall be liable for damages arising out of personal injuries and/or damage to real or tangible personal property of the State, employees of the State, persons designated by the State for training, or person(s) other than agents or employees of the Vendor, designated by the State for any purpose, prior to, during, or subsequent to delivery, installation, acceptance, and use of the Deliverables either at the Vendor's site or at the State's place of business, provided that the injury or damage was caused by the fault or negligence of the Vendor.

b) The Vendor agrees to indemnify, defend and hold the Agency and the State and its Officers, employees, agents and assigns harmless from any liability relating to personal injury or injury to real or personal property of any kind, accruing or resulting to any other person, firm or corporation furnishing or supplying work, services, materials or supplies in connection with the performance of this contract, whether tangible or intangible, arising out of the ordinary negligence, willful or wanton negligence, or intentional acts of the Vendor, its officers, employees, agents, assigns or subcontractors, in the performance of this Contract.

c) Vendor shall not be liable for damages arising out of or caused by an alteration or an attachment not made or installed by the Vendor, or for damage to alterations or attachments that may result from the normal operation and maintenance of the Vendor's goods.

32) General Indemnity: The Vendor shall hold and save the State, its officers, agents and employees, harmless from liability of any kind, including all claims and losses, with the exception of consequential damages, accruing or resulting from (1) any breaches of confidentiality, and/or (2) any actual or threatened third party claim for infringement of any third party intellectual property rights. The foregoing indemnification and defense by the Vendor shall be conditioned upon the following:

a) The Agency shall give Vendor written notice within thirty (30) days after it has actual knowledge of any such claim(s) or action(s) filed; and

b) The Vendor shall have the sole control of the defense of any such claim(s) or action(s) filed and of all negotiations relating to settlement or compromise thereof, provided, however, that the Agency or State shall have the option to participate at their own expense in the defense of such claim(s) or action(s) filed.

33) Changes: This Contract and subsequent purchase order(s) is awarded subject to shipment of quantities, qualities, and prices indicated by the order or Contract, and all conditions and instructions of the Contract or proposal on which it is based. Any changes made to this Contract or purchase order proposed by the Vendor are hereby rejected unless accepted in writing by the Agency or State Award Authority. The State shall not be responsible for Deliverables or services delivered without a purchase order from the Agency or State Award Authority.

34) Stop Work Order: The State may issue a written Stop Work Order to Vendor for cause at any time requiring Vendor to suspend or stop all, or any part, of the performance of Professional Services due under this Contract for a period up to ninety (90) days after the Stop Work Order is delivered to the Vendor. The ninety (90) day period may be extended for any further period for which the parties may agree.

a) The Stop Work Order shall be specifically identified as such and shall indicate that it is issued under this term. Upon receipt of the Stop Work Order, the Vendor shall immediately comply with its terms and take all reasonable steps to minimize incurring costs allocable to the work covered by the Stop Work Order during the period of work suspension or stoppage. Within a period of ninety (90) days after a Stop Work Order is delivered to Vendor, or within any extension of that period to which the parties agree, the State shall either:

i) Cancel the Stop Work Order, or

ii) Terminate the Professional Services covered by the Stop Work Order as provided for in the termination for default or the termination for convenience clause of this Contract.

b) If a Stop Work Order issued under this clause is canceled or the period of the Stop Work Order or any extension thereof expires, the Vendor shall resume the applicable Professional Services. The State shall make an equitable adjustment in the delivery schedule, the Contract price, or both, and the Contract shall be modified, in writing, accordingly, if:

i) The Stop Work Order results in an increase in the time required for, or in the Vendor's cost properly allocable to the performance of any part of this Contract, and

- ii) The Vendor asserts its right to an equitable adjustment within thirty (30) days after the end of the period of work stoppage; provided that if the State decides the facts justify the action, the State may receive and act upon a proposal submitted at any time before final payment under this Contract.
- c) If a Stop Work Order is not canceled and the work covered by the Stop Work Order is terminated in accordance with the provision entitled Termination for Convenience of the State, the State shall allow reasonable direct costs resulting from the Stop Work Order in arriving at the termination settlement.
- d) The State shall not be liable to the Vendor for loss of profits because of a Stop Work Order issued under this term.

35) Price Adjustments for Term Contracts: Reserved.

36) Time is of the Essence. Time is of the essence in the performance of this Contract.

37) Date and Time Warranty: The Vendor warrants that any Deliverable, whether hardware, firmware, middleware, custom or commercial software, or internal components, subroutines, and interface therein which performs any date and/or time data recognition function, calculation, or sequencing, will provide accurate date/time data and leap year calculations. This warranty shall survive termination or expiration of the Contract.

38) Independent Contractors: Vendor and its employees, officers and executives, and subcontractors, if any, shall be independent Vendors and not employees or agents of the State. This Contract shall not operate as a joint venture, partnership, trust, agency or any other business relationship.

39) Transportation: Transportation of tangible Deliverables shall be FOB Destination; unless otherwise specified in the solicitation document or purchase order. Freight, handling, hazardous material charges, and distribution and installation charges shall be included in the total price of each item. Any additional charges shall not be honored for payment unless authorized in writing by the Purchasing State Agency. In cases where parties, other than the Vendor ship materials against this order, the shipper must be instructed to show the purchase order number on all packages and shipping manifests to ensure proper identification and payment of invoices. A complete packing list must accompany each shipment.

40) Notices: Any notices required under this Contract should be delivered to the Contract Administrator for each party. Unless otherwise specified in the Solicitation Documents, any notices shall be delivered in writing by U.S. Mail, Commercial Courier or by hand.

41) Titles and Headings: Titles and Headings in this Contract are used for convenience only and do not define, limit or proscribe the language of terms identified by such Titles and Headings.

42) Amendment: This Contract may not be amended orally or by performance. Any amendment must be made in written form and signed by duly authorized representatives of the State and Vendor in conformance with Paragraph 33) (Changes) herein.

43) Taxes: The State of North Carolina is exempt from Federal excise taxes and no payment will be made for any personal property taxes levied on the Vendor or for any taxes levied on employee wages. Agencies of the State may have additional exemptions or exclusions for federal or state taxes. Evidence of such additional exemptions or exclusions may be provided to Vendor by Agencies, as applicable, during the term of this Contract. Applicable State or local sales taxes shall be invoiced as a separate item.

44) Governing Laws, Jurisdiction, and Venue:

a) This Contract is made under and shall be governed and construed in accordance with the laws of the State of North Carolina. The place of this Contract or purchase order, its situs and forum, shall be Wake County, North Carolina, where all matters, whether sounding in contract or in tort, relating to its validity, construction, interpretation and enforcement shall be determined. Vendor agrees and submits, solely for matters relating to this Contract, to the jurisdiction of the courts of the State of North Carolina, and stipulates that Wake County shall be the proper venue for all matters.

b) Except to the extent the provisions of the Contract are clearly inconsistent therewith, the applicable provisions of the Uniform Commercial Code as modified and adopted in North Carolina shall govern this

Contract. To the extent the Contract entails both the supply of "goods" and "services," such shall be deemed "goods" within the meaning of the Uniform Commercial Code, except when deeming such services as "goods" would result in a clearly unreasonable interpretation.

45) Force Majeure: Neither party shall be deemed to be in default of its obligations hereunder if and so long as it is prevented from performing such obligations as a result of events beyond its reasonable control, including without limitation, fire, power failures, any act of war, hostile foreign action, nuclear explosion, riot, strikes or failures or refusals to perform under subcontracts, civil insurrection, earthquake, hurricane, tornado, or other catastrophic natural event or act of God.

46) Compliance with Laws: The Vendor shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business, including those of federal, state, and local agencies having jurisdiction and/or authority. In providing Services and Deliverables, and without limiting or modifying in any respect the Vendor's obligations, Vendor shall comply, and shall cause each of its employees and subcontractors to comply at all times, with State policies that are of general application to State contractors or that Vendor has otherwise agreed to, comply with, including, without limitation, the Statewide Information Security Manual and ITS Security Standards and Policies.

47) State's Rights. All rights, duties and obligations under the Agreement inure to the State as a whole upon execution. The State's rights, duties and obligations under the Agreement shall continue without interruption notwithstanding any reorganization of State government in accordance with N.C.G.S. §143A-6.

48) Severability: In the event that a court of competent jurisdiction holds that a provision or requirement of this Contract violates any applicable law, each such provision or requirement shall be enforced only to the extent it is not in violation of law or is not otherwise unenforceable and all other provisions and requirements of this Contract shall remain in full force and effect. All promises, requirements, terms, conditions, provisions, representations, guarantees and warranties contained herein shall survive the expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable federal or State statute, including statutes of repose or limitation.

49) Federal Intellectual Property Bankruptcy Protection Act: The Parties agree that the Agency shall be entitled to all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto.

50) Electronic Procurement: Purchasing shall be conducted through the Statewide E-Procurement Service. The State's third party agent shall serve as the Supplier Manager for this E-Procurement Service. The Vendor shall register for the Statewide E-Procurement Service within two (2) business days of notification of award in order to receive an electronic purchase order resulting from award of this contract.

a) Reserved.

b) Reserved

c) The Supplier Manager will capture the order from the State approved user, including the shipping and payment information, and submit the order in accordance with the E-Procurement Service. Subsequently, the Supplier Manager will send those orders to the appropriate Vendor on State Contract. The State or State approved user, not the Supplier Manager, shall be responsible for the solicitation, bids received, evaluation of bids received, award of contract, and the payment for goods delivered.

d) Vendor agrees at all times to maintain the confidentiality of its user name and password for the Statewide E-Procurement Services. If a Vendor is a corporation, partnership or other legal entity, then the Vendor may authorize its employees to use its password. Vendor shall be responsible for all activity and all charges for such employees. Vendor agrees not to permit a third party to use the Statewide E-Procurement Services through its account. If there is a breach of security through the Vendor's account, Vendor shall immediately change its password and notify the Supplier Manager of the security breach by e-mail. Vendor shall cooperate with the state and the Supplier Manager to mitigate and correct any security breach.

51) Electronic Procurement (Applies only to Statewide Term Contracts): Reserved



**State of North Carolina
Office of Information Technology Services**

Pat McCrory
Governor

Chris Estes
State Chief Information Officer

To: Matt Dean
DocuSign, Inc.

From: Linda Waterman
OITS
Procurement

Subject: Amendment #3 – Amendment Request for OITS-006375
Initiate optional two (2) year renewal and change terms for renewal

Date: July 29, 2014

The Office of Information Technology Services (OITS) wishes to amend OITS-006375 to extend the agreement for two (2) years, as documented in the original award, and change the terms of the renewal. The term of this renewal shall be August 13, 2014 – August 12, 2016.

If you agree to this amendment, please sign the attached Amendment #3 and return for processing to this office by June 23, 2014. You may return the executed documents via fax to (919) 981-5374 or electronically via email to linda.waterman@nc.gov.

If you have any questions you may contact me at 919-754-6614 or via e-mail at linda.waterman@nc.gov.

DocuSign, Inc. / OITS Amendment #3 to OITS-006375

THIS AMENDMENT #3 ("Amendment #3") is entered into by and between DocuSign, Inc., 1301 2nd Avenue, Suite 2000, Seattle, Washington 98101, and Information Technology Services of 3700 Wake Forest Road, Raleigh, N.C. 27609 ("OITS").

The parties acknowledge: DocuSign and NCOSC entered into a contract, OITS-006375 August 13, 2012, for a period of two (2) years for \$777,800.00 (the "Agreement").

The parties acknowledge that a provision in the 2013-2015 North Carolina Budget Bill transferred the oversight of electronic signatures from the Office of the State Controller ("OSC") to the Office of Information Technology Services; Session Law 2013-360, s. 7.15(a). The transfer was effective July 1, 2013, and transition was completed October 1, 2013.

The parties acknowledge that Amendment #1 to the Agreement was executed on June 10, 2013.

The parties acknowledge that the first optional renewal of Connect Express ("Fetch") has been in place since August 12, 2013.

The parties acknowledge that the Agreement was amended February 28, 2014 ("Amendment #2") to acknowledge the transfer (assignment) of the Agreement from OSC to OITS and acknowledge the first optional renewal of Connect Express. The cost for this renewal was \$15,000.00.

The parties now agree in this Amendment #3 of the Agreement that The State of North Carolina Office of Information Technology Services and DocuSign, Inc. will renew the Agreement for an additional two (2) years in order to continue adoption of the current project and utilize existing Envelopes that have not been used. Currently, the residual Envelope Allowance is approximately 187,000 Envelopes in the Platform Subscription. There is no cost to the State for this renewal. Both parties agree that: (a) DocuSign will continue to provide pre-negotiated rates from the Agreement to organizations that are not approved by the NC Office of Information Technology Services for Envelopes covered by the initial Envelope Allowance of 200,000 Envelopes (See DocuSign Signed BAFO#2, pg 7, for rates); and (b) DocuSign will continue to offer Premier Support, provisioning assistance, training and onboarding assistance as outlined in the Agreement. The changes to the Agreement are as follows:

- DocuSign will be able to offer the unused Envelopes from the initial Envelope Allowance of 200,000 Envelopes to only Executive Branch agencies as identified by OITS.
 - If at a later date it is deemed necessary by OITS, the use of the envelopes may be expanded to include Higher Education, Community College System and Local Government.
- DocuSign will work with OITS to develop a plan for increasing DocuSign adoption within Executive Branch agencies.
- DocuSign will work with North Carolina to find a solution through a new contract model that addresses North Carolina's hopes of paying in arrears for Envelopes used by the State.
- On or before 8/1/2016, DocuSign and the State of North Carolina will negotiate a new agreement to assure the State additional future value in light of past contractual performance.

Except as amended herein, the Agreement remains in full force and effect as written. All pricing for products and services currently on contract, shall remain unchanged. Executed by authorized officials as of the day and date indicated below.

Vendor: DocuSign

**Office of Information Technology
Services**

BY: Loren Alhadeff Vice President - Corporate Sales

BY: _____

DocuSigned by:

Kristen Cullen

5BBA4219DE6D73F...

DocuSigned by:

Loren Alhadeff

Deputy State CIO

Office of Signer

Office of Signer

Aug-08-2014

8/11/2014 | 8:51:01 AM ET

Date of Execution

Date of Execution

DS
BAS

DS
CA

DS
LHD

DocuSign, Inc Amendment #4 to ITS-00006375

THIS AMENDMENT #4 is entered into by and between DocuSign, Inc., 1301 2nd Avenue, Suite 2000, Seattle Washington and the North Carolina Department of Information Technology of 3700 Wake Forest Road, Raleigh, N.C. 27609 (DIT).

The Parties acknowledge DocuSign and NC Officer of the State Controller (OSC) entered into a contract, ITS-006375 August 13, 2012 for a period of two (2) years for \$777,800.00.

Parties

The Parties acknowledge Amendment #1 was executed on June 10, 2013.

The Parties acknowledge the first optional renewal of Connect Express ("Fetch") was executed August 12, 2013.

The Parties acknowledge the Agreement was amended February 28, 2014 by Amendment #2 to acknowledge the transfer of this contract from OSC to DIT.

The Parties acknowledge the Agreement was amended August 8, 2014 continue the agreement for an additional two (2) years from August 13 2014 – August 12, 2016. (Amendment #3)

The Parties now agree to further amend the Agreement to extend the term of the Agreement for one (1) year from August 13, 2016 – August 12, 2017. The cost of this extension shall not exceed \$310,000.00 which includes a \$250,000 annual subscription fee. DIT retains the option to add \$60,000.00 of optional services should the State decide to utilize DocuSign as outlined in "Attachment A" and Exhibit "1".

The Parties acknowledge that Article 15 of Chapter 143B of the NC General Statutes, the Office of Information Technology Services is now the North Carolina Department of Information Technology

IRAN DIVESTMENT ACT: Pursuant to N.C.G.S. § 147-86.55 et seq., the State shall not enter into a contract unless the awarded Vendor provides a certification of compliance with the Iran Divestment Act to the awarding agency, and on a periodic basis thereafter as may be required by the State. Vendors are directed to review the foregoing laws. The State will provide the required certification to any awarded Vendor.

Except as amended herein, the Agreement remains in full force and effect as written. All pricing for products and services currently on contract, shall remain unchanged. Executed by authorized officials as of the day and date indicated below.

Vendor:
DocuSign, Inc

DIT:
Dept. of Information Technology

BY: DocuSigned by:
Catherine Chosh
C74C8351B7C84D8...

BY: DocuSigned by:
Keith Werner
72238681EB4F493

Sr. Manager, Revenue Operations

State CIO

Office of Signer

Office of Signer

June 17, 2016

6/27/2016 | 10:24 AM EDT

Date of Execution

Date of Execution

ATTACHMENT "A" FOR ITS 006375 Amendment 4

DocuSign eSignature Services

1. Amendment to ITS 006375: One (1) Year Agreement for a term of August 13, 2016 to August 12, 2017.
2. Purchase Order issued and Amendment to be executed prior to July 29, 2016
3. Annual Subscription: Annual DocuSign Platform Access and Support Fee = \$250,000.00.
 - Includes access to all features/functionality available on DocuSign platform (see Exhibit 1 for platform description)
 - Unlimited users
 - Enterprise Support Resources from DocuSign – Account Team, Dedicated Support Resources (Enterprise Account Manager, Technical Support Account Manager, Account Executive, Solutions Engineer)
4. All existing branches of NC State Government (Executive, Legislative and Judicial) may purchase envelope allowance subscriptions at any time during the amendment. These branches of government are covered under the DIT Annual Subscription and do not need to purchase their own platform fee.
5. All state universities, community colleges and technical schools may purchase envelope allowance subscriptions at any time during this amendment and do not need to purchase platform access.
6. Annual Envelopes:
 - Amendment to include: Extension on remaining approximately 120,000 envelopes remaining from original agreement as of July 31, 2016 – No additional purchase of envelopes required unless state transaction usage exceeds inventory during subscription.
 - The unused envelopes will be offered only to Executive Branch Agencies as identified by DIT.
 - Same tiered envelope pricing table as current contract for higher volumes:

Figure 1

Envelopes Purchased Annually	Cost per Envelope
10,000 – 49,999	\$0.55
50,000 -99,999	\$0.50
100,000 – 249,999	\$0.48
250,000 – 499,000	\$0.475
500,000 – 749,999	\$0.46
750,000 – 999,999	\$0.45
1,000,000 and above	\$0.43

7. Seat Purchases by State Agencies
 To date, only 63 seat licenses have been purchased. 50 have been by the higher education system and 13 by the Capital Workforce Development. DocuSign will honor the original contract pricing for these 63 seats for this One Year Amendment. No additional seats licenses will be available at the original contract pricing. Seat licensing is available to NC government customers at the current DocuSign edition prices (see Figure 2 below) they need for features/functionality requirements.
8. Existing cities and counties within the State of North Carolina that are current DocuSign customers as a result of the original agreement, will have the option to renew at a 7% increase to their current annual envelope allowance fee. For the life of this contract, these entities may renew their service with a maximum price increase of 7% year over year. Any new North Carolina City, County or K12 agency that wishes to purchase DocuSign can do so at the current DocuSign Public Sector User pricing per table below:

Figure 2 - User Subscription Pricing

DocuSign Edition	Annual Subscription Cost
Business Pro	\$470.40
Enterprise	\$1,019.20

9. Digital Transaction / eSignature Adoption Partnership: (Optional Services) Agency Adoption Accelerator - ½ time CSA (20 hours/week) – state purchases 3 months, get additional 3 months free. Six-month engagement in total with option to renew for 6 more months. Billed as consumed by state agencies or OIT. After 3 months, state will receive 3 months at no additional charge (exception is approved travel/expenses for requested onsite consulting).

- List Cost = \$204,000 plus T&E
- Discounted Cost = \$60,000 including T&E (up to 2 trips/month) (billed \$20,000/month in arrears)
- 3 Free Months = only T&E per terms and conditions listed in original agreement
- Renewal Option for 6 additional months

Features of DocuSign that are included for the State of North Carolina in this amendment

Category	Feature	Included/Option
Documents	Extensive File Type Support	Yes
	PDF Form Conversion	Yes
	20+ Customer/Standard Tags	Yes
	Cloud Storage Integration	Yes
	Automatic Tag Anchoring	Yes
	Powerforms	Yes
	Full Form Functionality	Yes
	Field Formatting	Yes
Data	Third-Party Data Fields	Yes
	Data Validation	Yes
	Field Logic	Yes
	Field & Document Markup	Yes
	DocuSign Connect	Yes
Workflow	Serial, Parallel & Mixed Routing	Yes
	Correct Documents	Yes
	Reminders & Notifications	Yes
	Templates	Yes
	Recipient Permissions	Yes
	Document Visibility Control	Yes
	Bulk Sending	Yes
Authentication	Email Based Authentication	Yes
	Geolocation Capture	Yes
	Social & 3 rd Party Authentication	Yes
	Access Code Authentication	Yes
	Federated Authentication (SSO)	Yes
Signature	Electronic Signature	Yes
	Express Digital Signatures	Yes
	Remote, In-Person, Mobile Signing	Yes
	Native Mobile Applications (IOS, Android and Windows)	Yes
	Accessibility	Yes
	Offline Signing and Sending	Yes
	Payment Processing	Yes
Reports	Real-Time Status	Yes
	Reports & Dashboards	Yes
	Data Export	Yes
Compliance	Tamper Sealed Documents	Yes
	Audit Trail	Yes
	Certificate of Completion	Yes
	Electronic Record Disclosure	Yes
	Watermarks	Yes
Retention	Email Archiving	Yes
	Document Retention Policies	Yes
	Document Custody Management	Yes
	Authoritative Copy	Yes
Configurable	Feature Access Control	Yes
	User and Access Controls	Yes
	Templates, Folders, Tags	Yes
	Organizational Branding	Multiple
	Password Policies	Yes
Integrations	Certified Partner Integrations	Yes
	CRM Connectors	Yes
	Single Sign On	Yes
	Custom API Integrations	Yes

DocuSign Envelope ID: CFC18713-8360-45E6-801B-4E65DD2C1E6E
DocuSign Envelope ID: 1A4E8DC5-BCCB-4B5C-B553-CBD30A2757FC

	Enterprise Development Sandbox	Yes
	Embedded Signing	Yes
Support	Dedicated Technical Support Mgr	Yes
	Dedicated Enterprise Account Team	Yes



DocuSign, Inc.
1301 2nd Avenue, Suite 2000
Seattle, WA 98101

Offer Valid Through: Jul 29, 2016
Prepared By: John Baldwin
Quote Number: Q-00140372

ORDER FORM

Address Information

Bill To:
State of North Carolina OITS
3512 Bush St
Raleigh, NC, United States 27609-7509

Ship To:
State of North Carolina OITS
3512 Bush St
Raleigh, NC, United States 27609-7509

Billing Contact Name:
Gordon Goeking
Billing Email Address:
gordon.goeking@nc.gov
Billing Phone:
(919) 754-6286

Shipping Contact Name:
Gordon Goeking
Shipping Email Address:
gordon.goeking@nc.gov
Shipping Phone:
(919) 754-6286

Order Details

Order Start Date: Aug 13, 2016
Order End Date: Aug 12, 2017
Billing Frequency: Upfront

Payment Method: Wire Transfer
Payment Terms: Net 30
Currency: USD

Products

Product Name	Start Date	End Date	Quantity	Net Price
DocuSign Platform Edition - Platform Fee	Aug 13, 2016	Aug 12, 2017	1	\$217,391.00
Premier Support	Aug 13, 2016	Aug 12, 2017	1	\$32,609.00
DocuSign System Automated Standard Edition - Envelope Subscription (Adoption Accelerator)	Aug 13, 2016	Aug 12, 2017	1	\$0.00

Grand Total: \$250,000.00

Product Details

Estimated Envelopes: 110,000
Seat Allowance: 1

Order Special Terms

For the Adoption Accelerator package(s) purchased in this Order Form, during the first 12 months of the Term, no overages charges shall apply for reasonable use of the Subscription Services that exceeds the specified Estimated Envelope Allowance.

Terms & Conditions

This Order Form covers the products and services described herein and is governed by the attached terms and conditions.

Billing Information

Prices shown above do not include any state and local taxes that may apply. Any such taxes are the responsibility of the Customer and will appear on the final invoice.

Is the contracting entity exempt from sales tax?

Please select Yes or No :

If yes, please send the required tax exemption documents immediately to taxexempt@docusign.com.

Invoices for this order will be emailed automatically from billing@docusign.com. Please make sure this email is on an approved setting or safe senders list so notifications do not go to a junk folder or caught in a spam filter.

Purchase Order Information

Is a Purchase Order (PO) required for the purchase or payment of the products on this Order Form?

Please select Yes or No :

If yes, please complete the following:

PO Number:

PO Amount: \$

By signing this Agreement, I certify that I am authorized to sign on behalf of the Subscriber and agree to the Terms and Conditions of this Order Form and any documents incorporated herein.

Subscriber

DocuSign, Inc.

Signature :

Signature :

Name :

Name :

Title :

Title :

Date :

Date :

DocuSign Envelope ID: 1A4E8DC5-BCCB-4B5C-B553-CBD30A2757FC

DocuSign, Inc Amendment #5 to ITS-00006375

THIS AMENDMENT #5 is entered into by and between DocuSign, Inc., 1301 2nd Avenue, Suite 2000, Seattle Washington and the North Carolina Department of Information Technology of 3700 Wake Forest Road, Raleigh, N.C. 27609 (DIT).

The Parties acknowledge DocuSign and NC Officer of the State Controller (OSC) entered into a contract, ITS-006375 August 13, 2012 for a period of two (2) years for \$777,800.00.

Parties

The Parties acknowledge Amendment #1 was executed on June 10, 2013.

The Parties acknowledge the first optional renewal of Connect Express ("Fetch") was executed August 12, 2013.

The Parties acknowledge the Agreement was amended February 28, 2014 by Amendment #2 to acknowledge the transfer of this contract from OSC to DIT.

The Parties acknowledge the Agreement was amended August 8, 2014 continue the agreement for an additional two (2) years from August 13 2014 – August 12, 2016. (Amendment #3)

The Parties acknowledge the Agreement was amended June 27, 2016 to extend the agreement for one (1) year for a period of August 13, 2016 – August 12, 2017 (Amendment #4)

The Parties now agree to further amend the Agreement to extend the term of the Agreement for one (1) year from August 13, 2017 – August 12, 2018. The cost of this extension is \$154,710.00, based on the pricing schedule below and will replace the pricing from the 2012 BAFO and include;

- 81,000 envelopes for shared use by Department of Transportation, Office of State Controller, Department of Information Technology, Community College System, Office of the Governor, Department of Public Safety, Veterans Affairs, Department of Environmental Quality, Department of Health and Human Services, Department of Public Instruction. Managed by the Department of Information Technology.
- The following DocuSign products and services; DocuSign Connector-Microsoft Dynamics CRM, DocuSign Connector – Microsoft SharePoint, DocuSign System Automation Premium Edition – Envelope Subscription, Premier Support.
- Overage fee of \$2.50 per envelope should additional envelopes not be purchased before current supply is exhausted.
- Additional Executive Branch Agencies, and other State and Local Governments desiring to utilize DocuSign would be able to purchase envelopes using this contract by contacting DIT via email or Remedy ticket to initiate communications with DocuSign and then will work directly with DocuSign to procure DocuSign envelopes to meet their business requirements. under the Terms and Conditions of this Agreement. These other Executive Branch Agencies, and other State and Local Governments will issue

their own purchase order and be responsible for envelopes costs under the following pricing schedule with a minimum purchase of 2,500 envelopes in a single transaction.

Number of Envelopes	Price Per Envelope
50,000 – 99,999	\$1.91
100,000 - 499,999	\$1.88
500,000 – 999,999	\$1.85
1,000,000 +	\$1.82

Additional updates to the Agreement;

1. DocuSign will complete the Iran Divestment Act Certification
IRAN DIVESTMENT ACT: Pursuant to N.C.G.S. § 147-86.55 et seq., the State shall not enter into a contract unless the awarded Vendor provides a certification of compliance with the Iran Divestment Act to the awarding agency, and on a periodic basis thereafter as may be required by the State. Vendors are directed to review the foregoing laws. The State will provide the required certification to any awarded Vendor.
2. **LEGISLATIVE MODIFICATIONS TO THE AGREEMENT.** DIT Terms and Conditions 22), 27), 31) and 30), found on pages 50, 52, and of the Original RFP (ITS-006375) are deleted and replaced as indicated below to conform to recently enacted legislation. (see SL 2016-85, which modified N.C.G.S. Chapter 143B to add N.C.G.S. §143B-1350(h1)).

22) Patent, Copyright, and Trade Secret Protection:

a) Vendor has created, acquired or otherwise has rights in, and may, in connection with the performance of Services for the State, employ, provide, create, acquire or otherwise obtain rights in various concepts, ideas, methods, methodologies, procedures, processes, know-how, techniques, models, templates and general purpose consulting and software tools, utilities and routines (collectively, the "Vendor Technology"). To the extent that any Vendor Technology is contained in any of the Deliverables including any derivative works, the Vendor hereby grants the State a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to use such Vendor Technology in connection with the Deliverables for the State's purposes; provided however that the parties acknowledge and agree Deliverables will not be construed to contain any Vendor software or proprietary technology.

b) Vendor shall not acquire any right, title and interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data or derivative works thereof, or other work products provided by the State to Vendor. The State hereby grants Vendor a royalty-free, fully paid, worldwide, perpetual, non-exclusive license for Vendor's internal use to non-confidential Deliverables first originated and prepared by the Vendor for delivery to the State.

c) The Vendor, at its own expense, shall defend any action brought against the State to the extent that such action is based upon a claim that the Services or other Deliverables supplied by the Vendor, or the operation of such Deliverables pursuant to a current version of Vendor-supplied software, infringes a patent, or copyright or violates a trade secret in the United States. The Vendor shall pay those costs and damages finally awarded against the State in any such action; damages shall be limited as provided in N.C.G.S. 143B-1350(h1). Such defense and payment shall be conditioned on the following:

- i) That the Vendor shall be notified within a reasonable time in writing by the State of any such claim; and,
- ii) That the Vendor shall have the sole control of the defense of any action on such claim and all negotiations for its settlement or compromise, provided, however, that the State shall

have the option to participate in such action at its own expense.

d) Should any Services or other Deliverable supplied by Vendor, or the operation thereof become, or in the Vendor's opinion are likely to become, the subject of a claim of infringement of a patent, copyright, or a trade secret in the United States, the State shall permit the Vendor, at its option and expense, either to procure for the State the right to continue using the goods/hardware or Software, or to replace or modify the same to become noninfringing and continue to meet procurement specifications in all material respects. If neither of these options can reasonably be taken, or if the use of such goods/hardware or Software by the State shall be prevented by injunction, the Vendor agrees to take back such goods/hardware or Software, and refund any sums the State has paid Vendor less any reasonable amount for use or damage and make every reasonable effort to assist the State in procuring substitute Deliverables. If, in the sole opinion of the State, the return of such infringing Deliverables makes the retention of other items of Deliverables acquired from the Vendor under this Contract impractical, the State shall then have the option of terminating the Contract, or applicable portions thereof, without penalty or termination charge. The Vendor agrees to take back such Deliverables and refund any sums the State has paid Vendor less any reasonable amount for use or damage.

e) Vendor will not be required to defend or indemnify the State if any claim by a third party against the State for infringement or misappropriation (i) results from the State's alteration of any Vendor-branded product or Deliverable, or (ii) results from the continued use of the good(s) or Services and other Deliverables after receiving notice they infringe a trade secret of a third party.

f) Nothing stated herein, however, shall affect Vendor's ownership in or rights to its preexisting intellectual property and proprietary rights.

27) Default: In the event Services or other Deliverable furnished or performed by the Vendor during performance of any Contract term fail to perform substantially in conformance with the documentation associated with the applicable Services, notice of the failure is provided by the State and if the failure is not cured within thirty (30) days, the State may cancel the contract. Default may be cause for debarment as provided in 09 NCAC 06B.1206. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.

a) If Vendor fails to deliver or provide correct Services or other Deliverables within the time required by this Contract, the State shall provide written notice of said failure to Vendor, and by such notice require performance assurance measures pursuant to N.C.G.S. 143B-1340(f). Vendor is responsible for the delays resulting from its failure to deliver or provide services or other Deliverables.

b) Should the State fail to perform any of its obligations upon which Vendor's performance is conditioned, Vendor shall not be in default for any delay, cost increase or other consequences resulting from the State's failure. Vendor will use reasonable efforts to mitigate delays, costs or expenses arising from assumptions in the Vendor's offer documents that prove erroneous or are otherwise invalid. Any deadline that is affected by any such failure in assumptions or performance by the State shall be extended by an amount of time reasonably necessary to compensate for the effect of such failure.

c) Vendor shall provide a plan to cure any delay or default if requested by the State. The plan shall state the nature of the delay or default, the time required for cure, any mitigating factors causing or tending to cause the delay or default, and such other information as the Vendor may deem necessary or proper to provide.

31) Limitation of Vendor's Liability:

a) Where Deliverables or Services are under the State's exclusive management and control, the Vendor shall not be liable for direct damages caused by the State's failure to fulfill any State responsibilities of assuring the proper use, management and supervision of the Deliverables and programs, audit controls, operating methods, office procedures, or for establishing all proper checkpoints necessary for the State's intended use of the Deliverables.

b) The Vendor's liability for damages to the State arising under the contract shall be limited to two times the value of the Contract.

c) The foregoing limitation of liability shall not apply to claims covered by other specific provisions including but not limited to Service Level Agreement or Warranty compliance, or to claims for injury to persons or damage to tangible personal property, gross negligence or willful or wanton conduct. This limitation of liability does not apply to contributions among joint tortfeasors under N.C.G.S. 1B-1 *et seq.*, the receipt of court costs or attorney's fees that might be awarded by a court in addition to damages after litigation based on this Contract.

Except as amended herein, the Agreement remains in full force and effect as written. All pricing for products and services currently on contract, shall remain unchanged. Executed by authorized officials as of the day and date indicated below.

Vendor:
DocuSign, Inc

DIT:
Dept. of Information Technology

DocuSigned by:
BY: Vinny Manrao
37DBA2FAAE824C8...

DocuSigned by:
BY: Tracy Doaks
EEADAC04EB804A2...

Vinny Manrao Manager, Revenue Operations

Tracy Doaks

Chief Deputy State CIO

Office of Signer

Office of Signer

August 15, 2017

8/15/2017 | 14:03:09 PM EDT

Date of Execution

Date of Execution



IRAN DIVESTMENT ACT CERTIFICATION

REQUIRED BY G.S. 147-86.59

1. As of the date written below, the undersigned certifies that:
 - a) He or she is authorized by DocuSign, Inc to make this certification, and
 - b) DocuSign, Inc, as a person defined in G.S. 147-86.57(6) is **not** currently identified by the State Treasurer pursuant to G.S. 147-86.58(1).

DocuSigned by:  Signature	August 15, 2017 Date
Nic Wolfe Printed Name	Corporate Counsel Title

Or:

2. As of the date written below, the undersigned certifies that:
 - a) He or she is authorized by [name of vendor] to make this certification, and
 - b) DocuSign, Inc, as a person defined in G.S. 147-86.57(6) is identified by the State Treasurer pursuant to G.S. 147-86.58(1).

Signature	Date
Printed Name	Title

And:

3. DocuSign, Inc claims an exception from the restrictions on State contracts under the Iran Divestment Act pursuant to G.S. 147-86.61, and submits relevant materials supporting its claim together with this Certification for the State's evaluation and consideration.

Signature	Date
Printed Name	Title

K. OTHER SUPPORTING MATERIAL INCLUDING TECHNICAL SYSTEM DOCUMENTATION

Questions from Addendum 3 – Q&A

After reviewing the Questions and Answers posted in Addendum 3, DocuSign addressed the issues within the individual answers. There were a few questions which weren't addressed in the body of our response, so they are provided below.

How often would data need to be transferred to internally hosted systems? Hourly? Daily?

DocuSign provides real-time data transfer capabilities through API calls to DocuSign or by subscribing to our DocuSign Connect Service. DocuSign Connect will push status/event updates to a 3rd party listener.

Any specific requirements for level of web content accessibility? I.e. WCAG 2.0A-AAA.

DocuSign is committed to providing our high-quality solution in a manner that is accessible to all individuals, regardless of their abilities. To meet this goal, DocuSign's accessibility support functionality provides all people equal access to and the freedom to interact with DocuSign's signing application when using assistive or adaptive technologies, in accordance with WCAG 2.0 Level AA and U.S. Government Section 508 standards.

- Web screen readers such as JAWS (Job Access With Speech), NVDA (NonVisual Desktop Access), ChromeVox, and VoiceOver with Safari
- Dragon Text to Speech
- Keyboard navigation
- Browser and signing experience zooming tools to provide low-visioned signers the ability to magnify documents without any loss of functionality.
- Tool tips and color contrast ratios for visually impaired signers.
- Finish button behavior. When signers select Finish the system performs validation and if any required fields have missing or incorrect data, the system will change the focus to that field and include information about what is wrong.
- Reading zones.

*Regarding uptime statistics, would the State prefer for vendors to provide the following metrics?
-Historical uptime for the last 3 months, 6 months, ad 12 months*

Carrier-grade Availability

DocuSign offers carrier-grade, "always on" availability. This means DocuSign has eliminated monthly maintenance (taking 0 minutes of planned downtime per year). We are a multi-year 99.99% operation. Please view the DocuSign Trust site (trust.docusign.com) for additional information.

Service	Service Level
Scheduled Uptime	24 hours per day, 7 days per week, 52 weeks per year
Subscription Service Availability	100%

Continuous Availability and Resilient Performance

Never worry about system availability or disaster recovery again.

- Carrier-grade Architecture
- Real-time replicating, active DocuSign sites
- Massively redundant distributed data (9 copies across 3 sites in North America or the EU)
- Fusion IO-powered, flash memory-based OLTP subsystem
- Global load balancing and traffic management with session-site based site failover



Benefits:

- Zero maintenance downtime
- Zero data loss in a disaster for maximum peace of mind
- Consistently high performance, even at peak load

DocuSign's Historical Uptime

While other vendors may claim a strong uptime, we invite the State to investigate our competitor's uptime records. Our closest competitor has frequently periods of downtime and large chunks of regularly scheduled maintenance. DocuSign is proud to report our historical uptime, which is the best in the industry.

- 2013 99.97% (does not include scheduled downtime)
- 2014 99.95% (last scheduled downtime was April 2014)
- 2015 99.9942%
- 2016 99.9954%
- 2017 99.9996% <https://trust.docusign.com/en-us/system-status/>

DocuSign provides a Trust Center to provide transparency into service performance, availability, and technical best practices. DocuSign's Trust Center is available here: <https://trust.docusign.com/>
A snap shot is provided below of the system status showing the last 12 months.

SOLICITATION # ITS-400335

ENVIRONMENTS	Uptime	Current Status	2018												2017			
			13	12	11	10	9	8	7	6	5	4	3	2	1	30	29	28
North America																		
NA1	100%																	
			2018						2017									
			Jun	May	Apr	Mar	Feb	Jan	Dec	Nov	Oct	Sep	Aug	Jul				
			100%	99.99%	100%	100%	100%	100%	100%	100%	100%	99.95%	100%	100%				
NA2	100%																	
			2018						2017									
			Jun	May	Apr	Mar	Feb	Jan	Dec	Nov	Oct	Sep	Aug	Jul				
			100%	100%	99.95%	99.99%	100%	100%	100%	99.99%	100%	100%	100%	100%				
NA3	100%																	
			2018						2017									
			Jun	May	Apr	Mar	Feb	Jan	Dec	Nov	Oct	Sep	Aug	Jul				
			100%	100%	100%	100%	100%	99.975%	100%	99.99%	99.99%	99.99%	100%	100%				
DEMO	100%																	
			2018						2017									
			Jun	May	Apr	Mar	Feb	Jan	Dec	Nov	Oct	Sep	Aug	Jul				
			100%	100%	100%	100%	100%	100%	99.99%	100%	100%	100%	100%	99.96%				
Europe																		
EU	100%																	
			2018						2017									
			Jun	May	Apr	Mar	Feb	Jan	Dec	Nov	Oct	Sep	Aug	Jul				
			100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	99.91%				
EU TSP	99.947%																	
Corporate																		
Headquarters	TBD																	
Customer Service	TBD																	
Learning Portal	100%																	

OK = OK = performance issue = service degradation

Previous three month's uptime

99.996%

Previous six month's uptime

99.996%

Previous 12 month's uptime

99.994%

-Uptime inclusive of maintenance windows

Yes, the reported uptime is inclusive of maintenance windows.

-Average hours the system is scheduled to be down for maintenance

DocuSign does not have scheduled maintenance windows. Our Carrier Grade Architecture is built to allow DocuSign to eliminate all scheduled maintenance of our system, which eliminated a full one hour of scheduled downtime per month.

DocuSign Policies and Procedures Worksheet

As you work to develop a IDIQ contract for the State, the following information on best practices in eSignature Policies and Procedures may be helpful. Please see the worksheets on the following pages.

DocuSign Policies & Procedures Design Worksheet

Objective

The purpose of this worksheet is to help build policies and Standard Operating Procedures for a comprehensive System of Agreement framework. Once you complete this worksheet, you will have a blueprint you can use to deploy DocuSign more quickly and efficiently.

Process

Conduct a first pass of this worksheet before you implement new use cases so that policy decisions can be rolled into the deployment. You can revisit these policies again once you're further along your digital transformation journey and ensure they align with your long-term vision.

Once you enact a policy or procedure, circulate this worksheet for review and approval by any relevant parties, such as:

- Your Company's DocuSign Center of Excellence (CoE)
- Legal team
- Security team
- IT Team
- Executive Sponsor

Policy Changes

These policies are not meant to be written in stone. They will evolve and become more efficient over time as use of DocuSign expands.

DocuSign product releases as well as customer releases that affect DocuSign can impact all policies and require revisions. Major organization changes would also prompt revisiting these policies.

About the Policies

This worksheet is broken out into two parts: 1) CORE Program Policies and 2) ANCILLARY Program Policies. CORE policies are critical to the DocuSign deployment and take priority as they impact ANCILLARY policies.



Table of Contents

Part 1: CORE Program Policies

- 1.1 - User Provisioning and Maintenance
- 1.2 - Account Provisioning and Maintenance
- 1.3 - Default DocuSign Account Settings and Compliance
- 1.4 - Sender and Signer Guidelines

Part 2: ANCILLARY Program Policies

- 2.1 - Enterprise-wide Support Process
- 2.2 - Enterprise-wide Training
- 2.3 - Enterprise-wide Reporting
- 2.4 - Enterprise-wide Document Archival
- 2.5 - Use Case Intake Process
- 2.6 - Enterprise-wide Deployment Process
- 2.7 - Enterprise-wide Template Maintenance Strategy
- 2.8 - Enterprise-wide Communication Plan
- 2.9 - DocuSign Program Health



Part 1: CORE Program Policies

1.1 - User Provisioning and Maintenance

Understand who your DocuSign users are. Define what they can do within your platform and how you will manage/control that access in a streamlined way.

	Questions	Responses
1.1.1	Who is authorized to provision new users in DocuSign?	
1.1.2	Who is authorized to have access to Organization Administration (enterprise-wide user mgmt., SSO config, Security appliance config, etc.)?	
1.1.3	Who is authorized to receive access to DocuSign?	
1.1.4	What permission profiles need to exist?	
1.1.5	What permission profile should new users be given by default?	
1.1.6	What criteria should determine when a user gets a non-default permission profile (Admin access, custom profile, etc.)?	
1.1.7	What groups should be created and which users should be added to them?	
1.1.8	What should the envelope sharing policy be?	
1.1.9	What process should be followed to request and grant a new user access or change access? - Account / Permission profile / Group / folder sharing access - User login addition / closures - Change requests	

Learn More:

- [Organization Administration](#)
- [Permission Profiles](#)
 - [Default Permission Profile settings](#)
- [Groups](#)
- [Envelope Sharing](#)



- How to Manage Users in DocuSign
- Best Practices for Delegated Administration
- An overview of Single Sign On

1.2 - Account Provisioning and Maintenance

Draft an architecture to organize your DocuSign usage. Consider ways to ensure that framework is adhered to. Exceptions should be considered but managed under the plan.

	Questions	Responses
1.2.1	When should a new DocuSign PROD account be created?	
1.2.2	When should a new DocuSign DEMO account be created?	
1.2.3	Who is authorized to request the creation of a new DocuSign PROD or DEMO account?	
1.2.4	What process should be followed to request the creation of a new DocuSign DEMO or PROD account?	
1.2.5	Who is authorized to request the closure of a new DocuSign PROD or DEMO account?	
1.2.6	What account should users be added to by default and when should users be added to an account other than the default?	

Learn More:

- Best practices around creating a Demo Account.
- Best practices around Change Management, specifically account management.

1.3 - Default DocuSign Account Settings and Compliance

Standardizing your DocuSign settings will 1) help your organization with future change management and troubleshooting by establishing a consistent baseline, and 2) ensure you remain compliant with any Legal or Security considerations.

Default permission profile information can be found in User Provisioning and Maintenance above.



	Questions	Responses
1.3.1	What should the naming convention of DocuSign accounts be?	
1.3.2	What branding should be used and under what scenarios?	
1.3.3	What default account settings should be used? Review ALL account settings, but specific areas of focus are: <ul style="list-style-type: none"> - Retention periods - Customized eDisclosure language - Specific verbiage required in Subject or email body. - Signer navigation - Signature adoption settings - Watermark - Attaching completed document to Completed email - Document visibility - Custody Transfer 	
1.3.4	What processes should be followed to ensure all accounts adhere to any required settings?	
1.3.5	If an account is allowed to change default account settings, how should that request be made and to whom?	

Learn More:

- Use the DocuSign [Admin Guide](#) for an overview of account settings
- [Branding](#)
- [Document Retention and Purging](#)

1.4 - Sender and Signer Guidelines

Define any processes that your users of DocuSign should follow to comply with Legal or Compliance.

	Questions	Responses
1.4.1	Under what scenarios are Senders allowed to use DocuSign (i.e. Countries, document types / categories, etc.)?	
1.4.2	Are there special authentication requirements that are required for certain Signers?	
1.4.3	What are the authentication requirements for Senders?	



1.4.4	If Signers are out of the office, what options can be offered to enable delegation?	
1.4.5	Are there any other requirements that Legal or Security/Compliance have for DocuSign Signers or Senders?	

Learn More:

- Review the eSignature [Legality Guide](#) which outlines legal considerations by Country
- [Legality of Electronic Signature in the US](#)
- An [overview](#) of the different authentication options for Signers
- Common features utilized in out-of-office management
 - [Envelope sharing](#)
 - [Correcting envelopes](#)
- SSO is a common Sender authentication method. Learn more [here](#).
- or use the technology out of fear they will get a massive un-forecasted bill at the end of the billing cycle. This has been shown to be an adoption inhibitor for early rollouts.

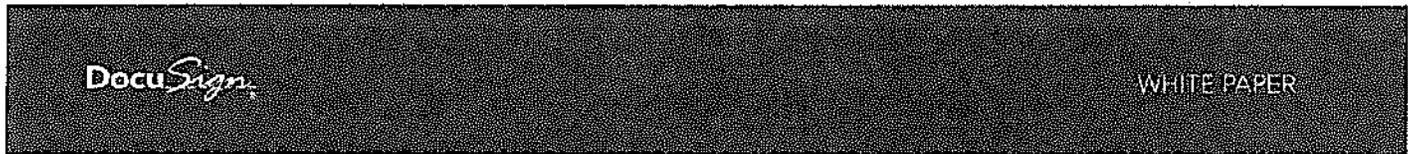
Part 2: ANCILLARY Program Policies

2.1 - Enterprise-wide Support Process

Ensure your DocuSign users have sufficient support to help them triage and resolve any of the following items:

- *Break/fix issues*
- *Account changes*
- *General "how-to" questions*

ID	Questions	Responses
2.1.1	What kinds of support issues will your Company handle yourselves and which ones should go to DocuSign?	
2.1.2	What is the desired triage process (Tier 1, Tier 2, etc.) for issues raised by DocuSign users?	
2.1.3	Who should communicate Support issues to DocuSign?	
2.1.4	What methods of communication should be used to communicate support issues within your Company?	



2.1.5	What methods of communication should be used to communicate support issues to DocuSign?	
2.1.6	DocuSign may send communication around Support-related topics your Company. Who should those communications go to?	

Learn More:

- Review DocuSign’s Support plans [here](#)
- DocuSign Success Plan for [Support](#)
- [DocuSign University’s “DocuSign Support for Customers”](#) self-paced learning course

2.2 - Enterprise-wide Training

Build a scalable training plan that provides your DocuSign users with the most relevant information in multiple learning formats.

	Questions	Responses
2.2.1	Who is responsible for training users on basic DocuSign signing and sending functionality?	
2.2.2	How will signing/sending training be conducted?	
2.2.3	Who is responsible for training DocuSign admins?	
2.2.4	How will admin training be conducted?	
2.2.5	Where will any self-help training material be published for future reference?	
2.2.6	What process should be followed to keep training information up-to-date?	
2.2.7	Do you want to offer custom training for individual use cases? If so, who should own this?	
2.2.8	When should you conduct DocuSign training?	

Learn More:

- DocuSign Success Plan on [Enablement](#)
- More about [DocuSign University](#)
- [Creating a DocuSign Portal](#)



2.3 - Enterprise-wide Reporting

You will have multiple audiences (Executive sponsors, managers/supervisors) interested in seeing DocuSign usage in a myriad of ways. Devise a strategy to intake and deliver these reports. Understand reporting needs up front as they can greatly impact how a use case should be built.

Question	Response
2.3.1 Who would like to see enterprise-wide reporting information?	
2.3.2 Who is responsible for gathering and sharing enterprise-wide reports?	
2.3.3 What process should be followed for gathering and sharing enterprise-wide reports?	
2.3.4 What information needs to be included in the enterprise-wide reports? Some examples include: <ul style="list-style-type: none"> - Envelope metadata - Form fields - History - User information - User stats 	
2.3.5 How should future reporting requests or changes be managed?	

Learn More:

- How to gather [Business Information and Insight](#)

2.4 - Enterprise-wide Document Archival

Keeping records of completed transactions for the appropriate amount of time and available to the right audience is paramount. Construct a process to handle these needs effectively. Understand archival needs up front as they can greatly impact how a use case should be built.

Question	Response
2.4.1 Where should completed documents from DocuSign go for long-term storage and retrieval?	
2.4.2 What process should be followed for archiving completed documents from DocuSign?	
2.4.3 Who owns and maintains the process / application used for document archival?	



2.4.4	How will you ensure that completed documents can be accessed by only authorized users?	
2.4.5	How should the Certificate of Completion be stored?	

Learn More:

- More about [DocuSign Retention and Purging](#)

2.5 - Use Case Intake Process

You may have multiple use cases in mind for DocuSign. Devise a process to organize those use cases into a roadmap, prioritize and add more as they arise.

QUESTION	RESPONSE
2.5.1	What method will be used to receive information about new use cases / users who are interested in using DocuSign?
2.5.2	What questions should be asked of each use case?
2.5.3	Describe the process to prioritize use cases for deployment (who, how often, criteria to consider).
2.5.4	What communication should be in place to disseminate the use case roadmap? And to whom?

Learn More:

- Review strategies for identifying and prioritizing use cases by [industry](#) or by [department](#)
- Leveraging [Use Case Intake Forms](#)
- Conducting a Digital Transaction Management [Assessment](#)
 - o [DTM Questionnaire](#)

2.6 - Use Case Deployment Process

Identify the key players and their roles to help deploy DocuSign use cases effectively.

QUESTION	RESPONSE
2.6.1	Who should own the use case deployment projects?
2.6.2	Who should be involved in the use case deployment projects?

2.6.3	How should the various project plans / timelines be communicated? And to whom?	
2.6.4	Who will build templates?	
2.6.5	What process must be followed to promote a use case to production (approvals, UAT, actual execution of transition steps, etc.)?	
2.6.6	What process should be followed to ensure the deployment was successful once it's fully live (e.g. follow-ups, end user feedback, ROI analysis, etc.)?	

Learn More:

- How Professional Services helps with deployments [here](#)
- [Use Case Deployment Toolkit](#)
- Deploying a Use Case [Worksheet](#)
- [Production Go-Live Checklist](#)
- Improving your [Adoption](#)
- [Web Application or API?](#)

2.7 - Enterprise-wide Template Maintenance Strategy

Some customer forms may be initiated by a broad user base. Generate a strategy that provides the right balance of control over the form requirements and autonomy for the senders to use or customize where appropriate.

Question	Responses
2.7.1 Who is responsible for building enterprise-wide templates?	
2.7.2 Who is responsible for maintaining enterprise-wide templates?	
2.7.3 What process should be followed for maintaining enterprise-wide templates and ensuring that all parties are using the most recent copy?	
2.7.4 Who needs to sign off on enterprise-wide templates before they can be used in Production?	
2.7.5 What protections should be placed on enterprise-wide templates to ensure integrity of use?	

Learn More:

- Best practices around [Change Management](#), specifically template management.



2.8 - Enterprise-wide Communication Plan

Devise a strategy to introduce the DocuSign program to your company and a methodical way to share program updates.

Support related communication is covered under Enterprise-wide Support Process.

	Questions	Responses
2.8.1	What types of mass communications do you want to send out regarding DocuSign?	
2.8.2	Who is the audience for mass communications?	
2.8.3	Who is responsible for crafting any mass communications?	
2.8.4	Who is authorized to send enterprise-wide communications regarding DocuSign?	

Learn More:

- [Leveraging Social Networks to Drive DocuSign Awareness and Adoption](#)
- [DocuSign Success Plan on Communication](#)
- [Communication Templates](#)



2.9 - DocuSign Program Health

Periodic check-ins of the overall program are critical to ensure long-term success. Executive sponsors, future team members of the DocuSign initiative, and DocuSign power users all benefit from this level of transparency.

Question	Responses
2.9.1 How often should parties come together to review the overall health of the DocuSign program?	
2.9.2 Who will lead the meeting and prepare the agenda?	
2.9.3 What information would the participants like to see?	
2.9.4 Where should program-level material be stored?	
2.9.5 Who should be responsible for overall program health, i.e. who is in the DS CoE)? What roles will they play?	

Learn More:

- Assess your program health [here](#)
- DocuSign Success Plan on [Governance](#)



Follow Us:

About DocuSign

DocuSign is changing how business gets done by empowering anyone to send, sign and manage documents anytime, anywhere on any device with trust and confidence. DocuSign and Go to keep life and business moving forward.

For U.S. inquiries: toll free 866-219-4318 | docuSign.com

©2015 DocuSign, Inc. All rights reserved. DocuSign, the DocuSign logo, the DocuSign logo for Digital Transaction Management, and the DocuSign logo for DocuSign are trademarks of DocuSign, Inc. The DocuSign logo for DocuSign, Inc. is a registered trademark of DocuSign, Inc. in the United States and other countries. All other trademarks and registered trademarks are the property of their respective owners.

K. TRAINING AND OTHER MATERIALS, SAMPLES OR EXAMPLES

Please reference section 19 Training of this response.

ATTACHMENTS

Solicitation

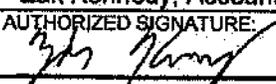
Please find the entire solicitation included in our response beginning on the following page.

STATE OF NORTH CAROLINA Department of Information Technology	REQUEST FOR PROPOSAL NO. ITS-400335	
	Offers will be publicly opened: July 12, 2018	
	Issue Date: June 11, 2018	
Refer ALL inquiries regarding this RFP to: Kristen Burnette kristen.burnette@nc.gov 919-754-6678	Commodity Number: 208	
	Description: Enterprise Electronic Forms and Digital Signature Capability	
	Using Agency: Multiple State Agencies	
See page 2 for mailing instructions.	Requisition No.: NA	

OFFER AND ACCEPTANCE: The State seeks offers for the Online Services and/or goods described in this solicitation. All offers and responses received shall be treated as offers to contract. The State's acceptance of any offer must be demonstrated by execution of the acceptance found below, and any subsequent Request for Best and Final Offer, if issued. Acceptance shall create a contract having an order of precedence as follows: Best and Final Offers, if any, Special terms and conditions specific to this RFP, Specifications of the RFP, the Department of Information Technology Terms and Conditions, and the agreed portion of the awarded Vendor's offer.

EXECUTION: In compliance with this Request for Proposal, and subject to all the conditions herein, the undersigned offers and agrees to furnish any or all Services or goods upon which prices are offered, at the price(s) offered herein, within the time specified herein. By executing this offer, I certify that this offer is submitted competitively and without collusion.

Failure to execute/sign offer prior to submittal shall render offer invalid. Late offers are not acceptable.

OFFEROR: Carahsoft Technology Corporation		
STREET ADDRESS: 1860 Michael Faraday Drive, Suite 100	P.O. BOX:	ZIP: 20190
CITY, STATE & ZIP: Reston, VA 20190	TELEPHONE NUMBER: 703-871-8500	TOLL FREE TEL NO 888-662-2724
PRINT NAME & TITLE OF PERSON SIGNING: Zak Kennedy, Account Representative		FAX NUMBER: 703-871-8505
AUTHORIZED SIGNATURE: 	DATE: 7/23/18	E-MAIL: Zak.Kennedy@carahsoft.com

Offer valid for ninety (90) days from date of offer opening unless otherwise stated here: ___ days.

ACCEPTANCE OF OFFER: If any or all parts of this offer are accepted, an authorized representative of AGENCY shall affix their signature hereto and this document and the documents identified above shall then constitute the written agreement between the parties. A copy of this acceptance will be forwarded to the awarded Vendor(s).

FOR AGENCY USE ONLY Offer accepted and contract awarded _____, as indicated on attached certification, by _____ (Authorized representative of DEPARTMENT OF INFORMATION TECHNOLOGY),

DELIVERY INSTRUCTIONS: The Vendor must deliver one (1) **signed original** and one (1) **copy** of the Offer to Issuing Agency in a sealed package with Company Name and RFP Number clearly marked on the front. **The Vendor must return all the pages of this solicitation in their response.** The Vendor must also submit one (1) signed, executed electronic copy of its offer on a USB Flash Drive(s). The files should not be password-protected and should be capable of being copied to other media.

Address envelope and insert offer number as shown below. Please note that the US Postal Service does not deliver any mail (US Postal Express, Certified, Priority, Overnight, etc.) on a set delivery schedule to this Office. **It is the responsibility of the Vendor to have the offer in this Office by the specified time and date of opening.**

DELIVER TO:
OFFER NUMBER: ITS-400335
Department of Information Technology
Attn: Kristen Burnette
3900 Wake Forest Road
Raleigh, NC 27609

Sealed offers, subject to the conditions made a part hereof, will be received at 3900 Wake Forest Road, Raleigh, NC 27609 until 2:00pm Eastern Standard Time on the day of opening and then opened, for furnishing and delivering the commodity as described herein. Offers must be submitted in a sealed package with the Execution page signed and dated by an official authorized to bind the Vendor's firm. Failure to return a signed offer shall result in disqualification. All offers must comply with Section VI, Proposal Content and Organization.

Offers will not be accepted by electronic means. This RFP is available electronically at <https://www.ips.state.nc.us/ips/>. All inquiries regarding the RFP specifications or requirements are to be addressed to the contact person listed on Page One.

NON-RESPONSIVE OFFERS: Vendor offers will be deemed non-responsive by the State and will be rejected without further consideration or evaluation if statements such as the following are included:

- "This offer does not constitute a binding offer",
- "This offer will be valid only if this offer is selected as a finalist or in the competitive range",
- "The Vendor does not commit or bind itself to any terms and conditions by this submission",
- "This document and all associated documents are non-binding and shall be used for discussion purposes only",
- "This offer will not be binding on either party until incorporated in a definitive agreement signed by authorized representatives of both parties", or
- A statement of similar intent.

VENDOR LICENSE OR SUPPORT AGREEMENT(S): The terms and conditions of the Vendor's standard services, license, maintenance or other agreement(s) applicable to Services, Software and other Products acquired under this RFP may apply to the extent such terms and conditions do not materially change the terms and conditions of this RFP. In the event of any conflict between the terms and conditions of this RFP and the Vendor's standard agreement(s), the terms and conditions of this RFP relating to audit and records, jurisdiction, choice of law, the State's electronic procurement application of law or administrative rules, the remedy for intellectual property infringement and the exclusive remedies and limitation of liability in the DIT Terms and Conditions herein shall apply in all cases and supersede any provisions contained in the Vendor's relevant standard agreement or any other agreement. The State shall not be obligated under any standard license and/or maintenance or other Vendor agreement(s) to indemnify or hold harmless the Vendor, its licensors, successors or assigns; nor arbitrate any dispute, nor pay late fees, legal fees or other similar costs.

DIGITAL IMAGING: The State will digitize the Vendor's response if not received electronically, and any awarded contract together with associated contract documents. This electronic copy shall be a preservation record, and serve as the official record of this solicitation with the same force and effect as the original written documents comprising such record. Any printout or other output readable by sight shown to reflect such record accurately is an "original."

QUESTIONS CONCERNING RFP: Written questions concerning this RFP will be received until June 21, 2018 at 2:00pm Eastern Standard Time. They must be sent via e-mail to: Kristen Burnette@nc.gov. Please insert "Questions ITS-400335" as the subject for the email. The questions should be submitted in the following format:

Citation	Vendor Question	The State's Response
Offer Section, Page Number		

The State will prepare responses to all written questions submitted, and post an addendum to the Interactive Purchasing System (IPS) <https://www.ips.state.nc.us/ips/>. Oral answers are not binding on the State.

Vendor contact regarding this RFP with anyone other than Kristen Burnette may be grounds for rejection of said Vendor's offer.

ADDENDUM TO RFP: If a pre-offer conference is held or written questions are received prior to the submission date, an addendum comprising questions submitted and responses to such questions, or any additional terms deemed necessary by the State will be posted to the Interactive Purchasing System (IPS), <https://www.ips.state.nc.us/ips/>, and shall become an Addendum to this RFP. Vendors' questions posed orally at any pre-offer conference must be reduced to writing by the Vendor and provided to the Purchasing Officer as directed by said Officer.

Critical updated information may be included in these Addenda. It is important that all Vendors bidding on this RFP periodically check the State website for any and all Addenda that may be issued prior to the offer opening date.

BASIS FOR REJECTION: Pursuant to 9 NCAC 06B.0401, the State reserves the right to reject any and all offers, in whole or in part; by deeming the offer unsatisfactory as to quality or quantity, delivery, price or service offered; non-compliance with the specifications or intent of this solicitation; lack of competitiveness; error(s) in specifications or indications that revision would be advantageous to the State; cancellation or other changes in the intended project, or other determination that the proposed specification is no longer needed; limitation or lack of available funds; circumstances that prevent determination of the best offer; or any other determination that rejection would be in the best interest of the State.

NOTICE TO VENDORS: The State may, but will not be required to evaluate or consider any additional terms and conditions submitted with an Offeror's response. This applies to any language appearing in or attached to the document as part of the Offeror's response. By execution and delivery of this Invitation for Offer and response(s), the Offer agrees that any additional terms and conditions, whether submitted purposely or inadvertently, shall have no force or effect unless such are specifically accepted by the State.

LATE OFFERS: Regardless of cause, late offers will not be accepted and will automatically be disqualified from further consideration. It shall be the Vendor's sole risk to ensure delivery at the designated office by the designated time. Late offers will not be opened and may be returned to the Vendor at the expense of the Vendor or destroyed if requested.

VENDOR REGISTRATION AND SOLICITATION NOTIFICATION SYSTEM: The NC electronic Vendor Portal (eVP) allows Vendors to electronically register with the State to receive electronic notification of current procurement opportunities for goods and Services available on the Interactive Purchasing System at the following web site: <https://www.ips.state.nc.us/ips>

POINTS OF CONTACT: Contact by the Offeror with the persons shown below for contractual and technical matters related to this RFP is only permitted if expressly agreed to by the procurement officer named on page 2, or upon award of contract:

Vendor Contractual Point of Contact	Vendor Technical Point of Contact
[NAME OF VENDOR] Street: [STREET ADDRESS] [CITY, STATE, ZIP] Attn: Assigned Contract Manager	[NAME OF VENDOR] Street: [STREET ADDRESS] [CITY, STATE, ZIP] Attn: Assigned Technical Lead

State Contractual Point of Contact	State Technical Point of Contact
North Carolina Department of Information Technology Statewide IT Procurement 3900 Wake Forest Road Raleigh, NC 27609 Attn: Kristen Burnette, Contract and Vendor Manager <u>kristen.burnette@nc.gov</u>	North Carolina Department of Information Technology 3700 Wake Forest Road Raleigh, NC 27609 Attn: Samila Mohseni, Enterprise Applications, Director <u>samila.mohseni@nc.gov</u>

Table of Contents

I. Introduction 6

II. Bidding Information 6

 A. Procurement Schedule 6

 B. Instructions to Vendors 7

 C. General Conditions for Proposals 8

 D. Evaluation Process 12

III. Technical Proposal 14

IV. Cost Proposal 31

V. Other Requirements and Special Terms 35

VI. Proposal Content and Organization 39

Attachment A. Attachments or Exhibits 42

Attachment B. Department of Information Technology Terms and Conditions 68

I. Introduction

The purpose of this Request for Proposal (RFP), and any resulting contract award, is for the North Carolina Department of Information Technology (NCDIT) on behalf of the State to solicit offers for an enterprise electronic forms and digital signature (EEF&DS) solution. Mandated by State Legislation, the awarded solution will replace North Carolina State Contract ITS006375 with a new multi-vendor/multi-solution statewide convenience contract. Contingent upon offer submissions, the State may choose to award one (1) or more Vendors as well as award multiple pricing models. The State's intent is to provide more than one cloud-based, software as a service (SaaS) solution that is responsive and cost effective to help state and local governments solve a wide variety of identity, authentication, confidentiality, data integrity, and non-repudiation (digital signatures) challenges. Multiple State agencies will leverage this contract, subsequently requiring the awarded vendor to invoice and provision each individual agency separately. Additionally, vendors should note that the State does require a rolled-up view of utilization both quarterly and yearly.

This state intends to award an *Indefinite Quantity Contract*, meaning this solicitation will establish a Contract pursuant to 9 NCAC 06B.0701 for an indefinite quantity contract between a vendor and the State. The quantity of goods or Services is undetermined. An estimated quantity based on past history or other means may be used as a guide, but shall not be a representation by the State of any anticipated purchase volume under any contract made pursuant to this solicitation.

In addition, the State reserves the right to make partial, progressive or multiple awards: where it is advantageous to award separately by items; or where more than one supplier is needed to provide the contemplated specifications as to quantity, quality, delivery, service, geographical areas; and where other factors are deemed to be necessary or proper to the purchase in question.

II. Bidding Information

A. Procurement Schedule

The Procurement Manager will make every effort to adhere to the following schedule:

Action	Responsibility	Date
Issue of RFP	Statewide IT Procurement	6/11/2018
Deadline to Submit Additional Questions	Potential Vendors	6/21/2018
Response to Written Questions/RFP Amendments	Department of Information Technology	6/28/2018
Submission of Offer	Vendor(s)	7/12/2018

Action	Responsibility	Date
Offer Evaluation Complete	Evaluation Committee	7/26/2018
Oral Presentation and/or Product Demonstrations by Finalists (optional)	Vendors	8/2/2018
Negotiations (optional)	Evaluation Committee designees and selected Vendor(s)	8/14/2018
Best and Final Offers from Finalists (optional)	Vendors	8/23/2018
Contract Award	IT Procurement Office	8/30/2018
Protest Deadline	Vendors	15 days after award

B. Instructions to Vendors

Additional acronyms, definitions and abbreviations may be included in the text of the RFP.

- 1) Offers submitted electronically, or via facsimile (FAX) machine will not be accepted.
- 2) **EXECUTION:** Failure to sign under EXECUTION section will render offer invalid.
- 3) **PROMPT PAYMENT DISCOUNTS:** Vendors are urged to compute all discounts into the price offered. If a prompt payment discount is offered, it will not be considered in the award of the Agreement except as a factor to aid in resolving cases of identical prices.
- 4) **MISCELLANEOUS:** Masculine pronouns shall be read to include feminine pronouns and the singular of any word or phrase shall be read to include the plural and vice versa.
- 5) **VENDOR REGISTRATION AND SOLICITATION NOTIFICATION SYSTEM:** Electronic Vendor Portal (eVP) allows Vendors to electronically register with the State to receive electronic notification of current procurement opportunities for goods and Services available on the Interactive Purchasing System at the following web site: <https://vendor.ncgov.com/vendor/login>
- 6) **ORGANIZATION:** Vendors are directed to carefully review Section VI herein and fully comply with the content and organizational requirements therein.
- 7) **E-PROCUREMENT:** This is not an E-Procurement solicitation. See paragraph #33 of the attached North Carolina Department of Information Technology Terms and Conditions Services made part of this solicitation contain language necessary for the implementation of North Carolina's statewide E-Procurement initiative. It is the Vendor's responsibility to read

these terms and conditions carefully and to consider them in preparing the offer. By signature, the Vendor acknowledges acceptance of all terms and conditions including those related to E-Procurement.

- a) General information on the E-Procurement service can be found at <http://eprourement.nc.gov/>
- b) Within two days after notification of award of a contract, the Vendor must register in NC E-Procurement @ Your Service at the following web site: <http://eprourement.nc.gov/Vendor.html>
- c) As of the RFP submittal date, the Vendor must be current on all E-Procurement fees. If the Vendor is not current on all E-Procurement fees, the State may disqualify the Vendor from participation in this RFP.

d) If the awarded Vendor does not stay current on all E-Procurement fees, the State may remove the Vendor from the Agreement for a thirty (30) calendar day period or until resolution, whichever is shorter. If the Vendor is making a reasonable effort to resolve any past due fees, no penalty will be imposed. The determination of the reasonable effort criteria will be at the discretion of the Statewide IT Procurement Office.

- 8) **E-VERIFY:** Pursuant to N.C.G.S. §143B-1350(k), the State shall not enter into a contract unless the awarded Vendor and each of its subcontractors comply with the E-Verify requirements of N.C.G.S. Chapter 64, Article 2. Vendors are directed to review the foregoing laws. Any awarded Vendor must submit a certification of compliance with E-Verify to the awarding agency, and on a periodic basis thereafter as may be required by the State.
- 9) **RESTRICTIONS ON CONTRACTS WITH THE STATE:** Reserved

C. General Conditions for Proposals

- 1) **DEFINITIONS, ACRONYMS AND ABBREVIATIONS:** Generally, see 9 NCAC 06A.0102 for definitions. The following are additional defined terms:
 - a) **24x7:** A statement of availability of systems, communications, and/or supporting resources every hour (24) of each day (7 days weekly) throughout every year for periods specified herein. Where reasonable downtime is accepted, it will be stated herein. Otherwise, 24x7 implies NO loss of availability of systems, communications, and/or supporting resources.
 - b) **ADA:** Americans with Disabilities Act
 - c) **APIs:** Application Programming Interfaces
 - d) **BAA:** Business Associates Agreement
 - e) **CRM:** Customer Relationship Management
 - f) **CSV:** Comma Separated Values
 - g) **Deliverables:** Deliverables, as used herein, shall comprise all Hardware, Vendor Services, professional Services, Software and provided modifications to any Software, and incidental materials, including any goods, Software or Services access license, data, reports and documentation provided or created during the performance or provision of Services hereunder. Deliverables include "Work Product" and means any expression of Licensor's findings, analyses, conclusions, opinions, recommendations, ideas, techniques, know-how, designs, programs, enhancements, and other technical information; but not source and object code or software.

- h) **EEF&DS:** Enterprise Electronic Forms and Digital Signature
 - l) **FERPA:** Family Educational Rights & Privacy Act
 - j) **Goods:** Includes intangibles such as computer software; provided, however that this definition does not modify the definition of "goods" in the context of N.C.G.S. §25-2-105 (UCC definition of goods).
 - k) **HIPAA:** Health Insurance Portability and Accountability Act
 - l) **IaaS:** Infrastructure as a Service
 - m) **IDM:** Identity Management
 - n) **LDAP:** Lightweight Directory Access Protocol
 - o) **NCID:** North Carolina Identity Service
 - p) **NCDIT or DIT:** The NC Department of Information Technology, formerly Office of Information Technology Services.
 - e) **ODBC:** Open Database Connectivity.
 - f) **Open Market Contract:** A contract for the purchase of goods or Services not covered by a term, technical, or convenience contract.
 - g) **PaaS:** Platform as a Service
 - h) **PII:** Personal Identifiable Information
 - i) **PCI:** Payment Card Industry
 - j) **Reasonable, Necessary or Proper:** as used herein shall be interpreted solely by the State of North Carolina.
 - k) **RFP:** Request for Proposal
 - l) **RPO:** Recovery Point Objective
 - m) **RTO:** Recovery Time Objective
 - n) **SaaS:** Software as a Service
 - o) **SLA:** Service Level Agreement
 - p) **SAP/SAP SSO:** Systems, Applications, and Products/ SAP Single Sign On
 - q) **The State:** Is the State of North Carolina, and its Agencies.
 - r) **Transaction:** Workflow package requiring one or more e-signatures.
 - s) **Vendor:** Company, firm, corporation, partnership, individual, etc., submitting an offer in response to a solicitation.
 - t) **WSI:** Web Services Interoperability
 - u) **NIEM:** National Information Exchange Model
- 2) **READ AND REVIEW:** It shall be the Vendor's responsibility to read this entire document, review all enclosures and attachments, and comply with all specifications and the State's intent as specified herein. If a Vendor discovers an inconsistency, error or omission in this solicitation, the Vendor should request a clarification from the State's contact person listed on the front page of the solicitation. Questions and clarifications must be submitted in writing and may be submitted by personal delivery, letter, fax or e-mail within the time period identified hereinabove.
- 3) **VENDOR RESPONSIBILITY:** The Vendor(s) will be responsible for investigating and recommending the most effective and efficient technical configuration for any online services. Consideration shall be given to the stability of the proposed configuration and the future direction of technology, confirming to the best of their ability that the recommended approach is not short lived. The Vendor(s) must provide a justification for their proposed online services solution(s) along with costs thereof. Vendors are encouraged to present explanations of benefits and merits of their proposed solutions together with any accompanying Services, maintenance, warranties, value

added Services or other criteria identified herein. The Vendor acknowledges that, to the extent the awarded contract involves the creation, research, investigation or generation of a future RFP or other solicitation, the Vendor will be precluded from bidding on the subsequent RFP or other solicitation and from serving as a subcontractor to an awarded vendor. The State reserves the right to disqualify any bidder if the State determines that the bidder has used its position (whether as an incumbent Vendor, or as a subcontractor hired to assist with the RFP development, or as a Vendor offering free assistance) to gain a competitive advantage on the RFP or other solicitation.

- 4) **ELIGIBLE VENDOR:** The Vendor certifies that in accordance with N.C.G.S. §143-59.1(b), the Vendor is not an ineligible vendor as set forth in N.C.G.S. §143-59.1 (a).
- 5) **ORAL EXPLANATIONS:** The State will not be bound by oral explanations or instructions given at any time during the bidding process or after award. Vendor contact regarding this RFP with anyone other than the Agency contact or procurement officer named on Page 1 above may be grounds for rejection of said Vendor's offer. Agency contact regarding this RFP with any Vendor may be grounds for cancellation of this RFP.
- 6) **INSUFFICIENCY OF REFERENCES TO OTHER DATA:** Only information that is received in response to this RFP will be evaluated. Reference to information previously submitted or Internet Website Addresses (URLs) will not suffice as a response to this solicitation.
- 7) **CONFLICT OF INTEREST:** Applicable standards may include: N.C.G.S. §§143B-1352 and 143B-1353, 14-234, and 133-32. The Vendor shall not knowingly employ, during the period of the Agreement, nor in the preparation of any response to this solicitation, any personnel who are, or have been, employed by a Vendor also in the employ of the State and who are providing Services involving, or similar to, the scope and nature of this solicitation or the resulting contract.
- 8) **CONTRACT TERM:** A contract awarded pursuant to this RFP shall have an effective date as provided in the Notice of Award. The term shall be **Three (3)** years, and will expire upon the anniversary date of the effective date unless otherwise stated in the Notice of Award, or unless terminated earlier. The State retains the option to extend the Agreement for **two (2)** additional **one (1)** year periods at its sole discretion.
- 9) **EFFECTIVE DATE:** This solicitation, including any Exhibits, or any resulting contract or amendment shall not become effective nor bind the State until the appropriate State purchasing authority/official or Agency official has signed the document(s), contract or amendment; the effective award date has been completed on the document(s), by the State purchasing official, and that date has arrived or passed. The State shall not be responsible for reimbursing the Vendor for Services rendered prior to the appropriate signatures and the arrival of the effective date of the Agreement. No contract shall be binding on the State until an encumbrance of funds has been made for payment of the sums due under the Agreement.
- 10) **RECYCLING AND SOURCE REDUCTION:** Reserved.

- 11) **HISTORICALLY UNDERUTILIZED BUSINESSES:** Pursuant to N.C.G.S. §§143B-1361(a), 143-48 and 143-128.4 and any applicable Executive Order, the State invites and encourages participation in this procurement process by businesses owned by minorities, women, disabled, disabled business enterprises and non-profit work centers for the blind and severely disabled. Additional information may be found at: <http://ncadmin.nc.gov/businesses/hub/>.
- 12) **CLARIFICATIONS/INTERPRETATIONS:** Any and all amendments or revisions to this document shall be made by written addendum from the DIT Procurement Office. Vendors may call the purchasing agent listed on the first page of this document to obtain a verbal status of contract award. If either a unit price or extended price is obviously in error and the other is obviously correct, the incorrect price will be disregarded.
- 13) **RIGHTS RESERVED:** While the State has every intention to award a contract as a result of this RFP, issuance of the RFP in no way constitutes a commitment by the State of North Carolina, or the procuring Agency, to award a contract. Upon determining that any of the following would be in its best interests, the State may:
- a) waive any formality;
 - b) amend the solicitation;
 - c) cancel or terminate this RFP;
 - d) reject any or all offers received in response to this RFP;
 - e) waive any undesirable, inconsequential, or inconsistent provisions of this RFP;
 - f) if the response to this solicitation demonstrate a lack of competition, negotiate directly with one or more Vendors;
 - g) not award, or if awarded, terminate any contract if the State determines adequate State funds are not available;
 - h) if all offers are found non-responsive, determine whether Waiver of Competition criteria may be satisfied, and if so, negotiate with one or more known sources of supply 09 NCAC 06B.0316 (c); or
 - i) negotiate with one or more Vendors under 09 NCAC 06B.0316 (b).
- 14) **ALTERNATE OFFERS:** The Vendor may submit alternate offers for various levels of Service(s) meeting specifications. Alternate offers must specifically identify the RFP specifications and advantage(s) addressed by the alternate offer. Any alternate offers must be clearly marked with the legend as shown herein. Each offer must be for a specific set of Services and offer at specific pricing. If a Vendor chooses to respond with various Services offerings, each must be an offer with a different price and a separate RFP offer.

Alternate offers must be clearly marked

“Alternate Offer for ‘name of Vendor’”

and numbered sequentially with the first offer if separate offers are submitted. This legend must be in bold type of not less than 14-point type on the face of the offer, and on the text of the alternative offer.

- 15) **CO-VENDORS:** Vendors may submit offers as partnerships or other business entities. Such partners or other “co-Vendors”, if any, shall disclose their

relationship fully to the State. The State shall not be obligated to contract with more than one Vendor. Any requirements for references, financial statements or similar reference materials shall mean all such partners or co-Vendors.

- 16) **SUBMITTING AN OFFER:** Each Vendor submitting an offer warrants and represents that:
 - a) The offer is based upon an understanding of the specifications and requirements described in this RFP.
 - b) Costs for developing and delivering responses to this RFP and any subsequent presentations of the offer as requested by the State are entirely the responsibility of the Vendor. The State is not liable for any expense incurred by the Vendors in the preparation and presentation of their offers.
- 17) **SUBMITTED MATERIALS:** All materials submitted in response to this RFP become the property of the State and are to be appended to any formal documentation, which would further define or expand any contractual relationship between the State and the Vendor resulting from this RFP process.
- 18) **MODIFICATIONS TO OFFER:** An offer may not be unilaterally modified by the Vendor.

D. Evaluation Process

- 1) **BEST VALUE:** "Best Value" procurement methods are authorized by N.C.G.S. §§143-135.9 and 143B-1350(h). The award decision is made based on multiple factors, including: total cost of ownership, meaning the cost of acquiring, operating, maintaining, and supporting a product or service over its projected lifetime; the evaluated technical merit of the Vendor's offer; the Vendor's past performance; and the evaluated probability of performing the specifications stated in the solicitation on time, with high quality, and in a manner that accomplishes the stated business objectives and maintains industry standards compliance. The intent of "Best Value" Information Technology procurement is to enable Vendors to offer and the Agency to select the most appropriate solution to meet the business objectives defined in the solicitation and to keep all parties focused on the desired outcome of a procurement. Evaluation shall also include compliance with information technology project management policies, compliance with information technology security standards and policies, substantial conformity with the specifications, and other conditions set forth in the solicitation.
- 2) **SOURCE SELECTION:** A trade-off/ranking method of source selection will be utilized in this procurement to allow the State to award this RFP to the Vendor providing the Best Value, and recognizing that Best Value may result in award other than the lowest price or highest technically qualified offer. By using this method, the overall ranking may be adjusted up or down when considered with, or traded-off against other non-price factors.
 - a) The evaluation committee may request clarifications, an interview with or presentation from any or all Vendors as allowed by 9 NCAC 06B.0307. However, the State may refuse to accept, in full or partially, the response to a clarification request given by any Vendor. Vendors are cautioned that the evaluators are not required to request clarifications; therefore, all offers should be complete and reflect the most favorable terms. Vendors should

be prepared to send qualified personnel to Raleigh, North Carolina, to discuss technical and contractual aspects of the offer.

- b) **Evaluation Process Explanation.** State Agency employees will review all offers. All offers will be initially classified as being responsive or non-responsive. If an offer is found non-responsive, it will not be considered further. All responsive offers will be evaluated based on stated evaluation criteria. Any references in an answer to another location in the RFP materials or Offer shall have specific page numbers and sections stated in the reference.
 - c) To be eligible for consideration, a Vendor's offer must substantially conform to the intent of all specifications. Compliance with the intent of all specifications will be determined by the State. Offers that do not meet the full intent of all specifications listed in this RFP may be deemed deficient. Further, a serious deficiency in the offer to any one factor may be grounds for rejection regardless of overall score.
 - d) Vendors are advised that the State is not obligated to ask for, or accept after the closing date for receipt of offer, data that is essential for a complete and thorough evaluation of the offer.
- 3) **BEST AND FINAL OFFERS (BAFO):** If negotiations or subsequent offers are solicited, the Vendors shall provide BAFOs in response. Failure to deliver a BAFO when requested shall disqualify the non-responsive Vendor from further consideration. The State may establish a competitive range based upon evaluations of offers, and request BAFOs from the Vendors within this range; e.g. "Finalist Vendors". The State will evaluate BAFOs and add any additional weight to the Vendors' respective offer. Additional weight awarded from oral presentations and product demonstrations during negotiations, if any, will be added to the previously assigned weights to attain their final ranking.
- 4) **EVALUATION CRITERIA:** Each of the criteria below shall be evaluated in accordance with the solicitation documents:
- a) **Corporate Background and Experience:** Vendor's corporate background and similar experience specifically relevant to the technical situations, specifications, needs, challenges, and opportunities as presented in this RFP.
 - b) **Technical Approach:** Substantial Conformity to Solicitation Requirements and Specifications;
 - i. Effectiveness of approaches, designs, services, processes, and practices as they relate to the solution.
 - ii. Illustration(s) and/or explanations of the Statewide Technical Architecture objectives, principles and best practices to the proposed solution.
 - c) **Proposed Approach and Schedule:** Proposed approach and schedule of work to be performed. This encompasses areas such as producing acceptable deliverables; organization, timing, and structure of work activities in accordance with any stated timeframes.
 - d) **Total Cost of Ownership:** The cost of acquiring, operating, maintaining, and supporting a product or service over its projected lifetime.

- 5) **PAST PERFORMANCE:** Vendor may be disqualified from any evaluation or award if Vendor or any key personnel proposed, has previously failed to perform satisfactorily during the performance of any contract with the State, or violated rules or statutes applicable to public bidding in the State.
- 6) **EVALUATION METHOD:** This procurement will be evaluation in accordance with the Narrative method.
- 7) **INTERACTIVE PURCHASING SYSTEM (IPS):** The State has implemented links to the Interactive Purchasing System (IPS) that allow the public to retrieve offer award information electronically from our Internet web site: <https://www.ips.state.nc.us/ips/>. Click on the IPS BIDS icon, click on Search for BID, enter the Agency prefix-offer number (XXXX), and then search. This information may not be available for several weeks dependent upon the complexity of the acquisition and the length of time to complete the evaluation process.
- 8) **PROTEST PROCEDURES:** Protests of awards exceeding \$25,000 in value must be submitted to the issuing Agency at the address given on the first page of this document. Protests must be received in this office within fifteen (15) calendar days from the date of this RFP award and provide specific reasons and any supporting documentation for the protest. **All protests will be governed by Title 9, Department of Information Technology (formerly Office of Information Technology Services), Subchapter 06B Sections .1101 - .1121.**

III. Technical Proposal

- 1) **ENTERPRISE ARCHITECTURE STANDARDS:** The North Carolina Statewide Technical Architecture is located at the following website: (<https://it.nc.gov/services/it-architecture/statewide-architecture-framework>). This provides a series of domain documents describing objectives, principles and best practices for the development, implementation, and integration of business systems. Agencies and Vendors should refer to these Architecture documents when implementing enterprise applications and/or infrastructure.
- 2) **ENTERPRISE LICENSING:** In offering the best value to the State, Vendors are encouraged to leverage the State's existing resources and license agreements. The agreements may be viewed at: <http://it.nc.gov/services/license-and-agreements>
 - a) Identify components or products that are needed for your solution that may not be available with the State's existing license agreement.
 - b) Identify and explain any components that are missing from the State's existing license agreement.
 - c) If the Vendor can provide a more cost effective licensing agreement, please explain in detail the agreement and how it would benefit the State.
 - d) Explain the transportability and transferability of the proposed license agreements. Any licenses or warranties purchased on behalf of the State for this project must be transferable at the time the Vendor is paid under contract for said component
- 3) **VIRTUALIZATION:** *Reserved*

- 4) **NCID:** Reserved.
- 5) **CLOUD SERVICE PROVIDERS (CSPs):** For offers featuring a cloud-hosted solution, Vendors shall describe how the proposed solution will support the agency's information system security compliance requirements as described in the Statewide Information Security Manual, specifically relating to, and without limitation, the sections relating to cloud services: <http://it.nc.gov/statewide-resources/policies>. *The e-Forms/e-Signature Program should be classified as NIST Moderate per the Statewide Information Security Manual and will be required to receive and securely manage data that is classified up to Restricted or Highly Restricted per the State's Data Classification and Handling Policy.* To comply with policy, State agencies are required to perform annual security/risk assessments on their information systems using NIST 800-53 controls. This requirement additionally applies to all vendor provided, agency managed Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions. Assessment reports such as the Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, and ISO 27001 are preferred and offered solutions already meeting these requirements are requested to include these reports as part of their submission.
- 6) **BRANDING:** All offers that incorporate State design and branding, as specified by the State, shall adhere to the State style guide. The State style guide is located at: <http://digitalstyle.nc.gov>.
- 7) **EQUIVALENT ITEMS:** Reserved.
- 8) **LITERATURE:** All offers shall include specifications and technical literature sufficient to allow the State to determine that the proposed solution substantially meets all specifications. This technical literature will be the primary source for evaluation. If a specification is not addressed in the technical literature it must be supported by additional documentation and included with the offer. Offer responses without sufficient technical documentation may be rejected.
- 9) **EQUIVALENT GOODS:** Reserved.
- 10) **DEVIATION FROM SPECIFICATIONS:** Any deviation from specifications indicated herein must be clearly identified as an exception and listed on a separate page labeled "Exceptions to Specification." Any deviations shall be explained in detail. **The Vendor shall not construe this paragraph as inviting deviation or implying that any deviation will be acceptable. Offers of alternative or non-equivalent goods or services may be rejected if not found substantially conforming; and if offered, must be supported by independent documentary verification that the offer substantially conforms to the specified goods or services specification.**
- 11) **SCOPE OF WORK:**
In 2013, the General Assembly transferred the responsibility of procuring electronic forms and digital signature services from the Office of the State Controller (OSC) to the Department of Information Technology (DIT) and the agency's State CIO. Thereby, per North Carolina State Legislation, the

awarded solution must adhere to several technical requirements (**Please see Section III, #12.**)

The following language is taken directly from the North Carolina statute:

The proposed digital solution shall adhere to the N.C. Uniform Electronic Transactions Act (NCGS 66311), the Federal Electronic Signatures in Global and National Commerce Act (Title 15), NC eCommerce (NCGS 66-58.12), NC Cash Management Statute (NCGS 147.86-22(b)), and the Electronic Notary Act (Chapter 10B, Article 2) and the N.C. Electronic Notary Standards (18 NCAC 07C) § 66-58.4. Use of electronic signatures.

All public agencies may use and accept electronic signatures pursuant to this Article, pursuant to Article 40 of this Chapter (the Uniform Electronic Transactions Act), or pursuant to other law. (1998-127, s. 1; 2003-233, s. 1; 2007-119, s. 1.)

Based on current usage, the State estimates that the solution will eventually accommodate over 95,000 transactions. The State will proceed with a decentralized approach of the program with minimal central management of the enterprise form and digital signature solution. This approach will allow the State to enter into contracts with vendors and allow agencies to access services as they need them for the most cost-effective price. Therefore, in addition to solving a wide variety of identity, authentication, confidentiality, data integrity, and non-repudiation (digital signatures) challenges, any vendor partnerships must invoice and provision each individual agency separately.

12) **TECHNICAL REQUIREMENTS:**

In accordance with the legislative mandate, the awarded solution must conform with the following requirements. Vendors should read the information regarding each requirement and any corresponding reference, and provide detailed answers when prompted. Note: Solutions not adhering to technical requirements will not be considered by the State.

a) **PII (Personal Identifiable Information)**

N.C. Gen. Stat. §75-61(10) defines personal identifying information (PII), in part, as "[a] person's first name or first initial and last name in combination with identifying information as defined in G.S. 14-113.20(b)," and "identifying information" is defined by G.S. § 14-113.20(b) to include Social Security Number or employer taxpayer identification numbers, Driver's License, State Identification Card, or Passport Numbers, Checking Account Numbers, Savings Account Numbers, Credit Card Numbers, Debit Card Numbers, Personal Identification (PIN) Code as defined in G.S. § 14-113.8(6), Electronic identification numbers, electronic mail names or addresses, internet account numbers, or Internet identification names, Digital Signatures, any other numbers or information that can be used to access a person's financial resources, Biometric Data, Fingerprints, Passwords and Parents' legal surnames prior to marriage. **Proposed solutions must adhere to PII protection laws.**

Therefore, please describe how the solution is PII compliant.

b) HIPAA (Health Insurance Portability and Accountability Act)

The Contractor agrees that, if the Division determines that some or all of the activities within the scope of this contract are subject to the Health Insurance Portability and Accountability Act of 1996, P.L. 104-91, as amended ("HIPAA"), or its implementing regulations, it will comply with the HIPAA requirements and will execute such agreements and practices as the Division may require to ensure compliance. HIPAA forms, instructions and other materials can be located on the HIPAA web site: <http://hipaa.dhhs.state.nc.us/index.html>. **If applicable, proposed solutions must adhere to HIPAA laws.**

In consideration of this requirement, please describe how the proposed solution is HIPAA compliant. Please note that the State requires a business associates agreement (BAA).

c) PCI (Payment Card Industry)

The Payment Card Industry (PCI) Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.

In consideration of this requirement, please describe how the proposed solution is PCI compliant.

d) FERPA (Family Educational Rights & Privacy Act)

The Family Educational Rights & Privacy Act (FERPA) states that student educational records are subject to 20 U.S.C. 1232g, Family Rights and Privacy Act (FERPA). Therefore, the Vendor must ensure that the proposed solution fully complies with FERPA and every employee responsible for carrying out the terms of this contract is aware of the confidentiality requirements of federal law. In addition, every such employee must sign a confidentiality acknowledgement that indicates that he or she understands the legal requirements for confidentiality. The Vendor is responsible for the actions of its employee and must take all precautions necessary to ensure that no violations occur. Finally, access to personally identifiable student education information shall be limited to those employees who must have access to it in order to perform their responsibilities pursuant to this contract.

In compliance with the law, please describe the following:

1. Describe the capabilities of tracking and reporting the application access.
2. Describe the solution's approach to handling non-public data at rest and non-public data in motion.
3. Describe the solution's approach for encrypting data such that only the intended recipient can decrypt it.
4. Describe the solution's process for handling and notification of a breach of non-public data.
5. For authorization, describe the solution's handling of various roles associated with data access.

e) **Security**

The state potentially handles a large amount of non-public data. **Proposed solutions must adhere to North Carolina Statewide IT Security Policies and Standards (<https://it.nc.gov/statewide-information-security-policies>), as they may relate to personal and/or confidential data.** Therefore, please address the following:

The State also requires that all systems connected to the State network or process State data, meet an acceptable level of security compliance. This includes those systems that operate outside of the States' direct control such as Cloud Services defined as Software as a Service (SaaS), Infrastructure as a Service (IaaS) or Platform as a Service (PaaS). **Attachment B** provides a high-level view of specific security requirements that are requirements to meet compliance. Vendors must fill out the **VENDOR ASSESSMENT GUIDE in Attachment B**.

Note: There may be additional requirements depending on the sensitivity of the data and other Federal and State mandates.

The following items are security and/or solution requirements; therefore, describe how the solution will accommodate the following:

1. The solution must alert the user to any changes to a document after a digital signature has been applied.
2. The digital signature service component must require users to prove their identity before applying an electronic signature to a document.
3. The solution must provide digital certificates to establish non-reputation (i.e. cannot deny receipt or signature).
4. The solution must provide digital hashes to establish fixity (i.e. guarantees that digital documents have not been altered since completion).

13) **TECHNICAL SPECIFICATIONS:** Means, as used herein, a specification that documents the requirements of a system or system component. It typically includes functional requirements, performance requirements, interface requirements, design requirements, development standards, maintenance

standards, or similar terms. Substantial conformity with technical specifications is required.

- a) **Site and System Preparation:** Vendors shall provide the Purchasing State Agency complete site requirement specifications for the Deliverables, if any. These specifications shall ensure that the Deliverables to be installed or implemented shall operate properly and efficiently within the site and system environment. The Vendor shall advise the State of any site requirements for any Deliverables required by the State's specifications. Any alterations or modification in site preparation which are directly attributable to incomplete or erroneous specifications provided by the Vendor and which would involve additional expenses to the State, shall be made at the expense of the Vendor.
- b) **Specifications:** The apparent silence of the specifications as to any detail, or the apparent omission of detailed description concerning any point, shall be regarded as meaning that only the best commercial practice is to prevail and only processes, configuration, material and workmanship of the first quality may be used. Upon any notice of noncompliance provided by the State, Vendor shall supply proof of compliance with the specifications. Vendor must provide written notice of its intent to deliver alternate or substitute Services, products, goods or other Deliverables. Alternate or substitute Services, products, goods or Deliverables may be accepted or rejected in the sole discretion of the State; and any such alternates or substitutes must be accompanied by Vendor's certification and evidence satisfactory to the State that the function, characteristics, performance and endurance will be equal or superior to the original Deliverables specified. See, Acceptance Criteria, below.
- c) **Directions:** Please describe how the proposed solution will meet the following technical specifications, including capabilities, features, and limitations. *Note: Vendors are encouraged to align responses with the technical specifications' outline shown below.*

1. General Features

Provide the general features of the proposed solution. Please include the following information:

- a. Use this prompt to articulate an understanding of the state's need as well as any value-added services relevant to this RFP.
- b. Address the solution's capacity to include ad hoc workflow routing rules, based on unique business rules defined for document(s) and signature requirements.
- c. Can the solution deliver business process workflow for documents, from originator to signatories?
- d. Can the solution integrate with global address books or pull users into a centralized address book?
- e. Address whether the solution will permit external party signing, including two-factor or multi-factor authentication. Provide examples.
- f. Describe the capability to establish evidentiary requirements for signed documents.
- g. Describe the process of creating new forms and templates.

- h. Address whether each person in the workflow is given the opportunity to review all documents, with confirmation opportunity, before the transaction continues.
- i. The State needs the signing process to be simple, and require very few steps for users. The steps required to secure signatures should not become more burdensome for any staff involved than current paper processes. Therefore, describe if the solution configures predefined workflow routing rules based on specific business rules defined for document(s) and signature requirements.
- j. Describe the solution's capacity to store completed, digitally signed document(s), on the State's own Document Management System; Include whether the:
 - Solution supports grouping and/or compartmentalization of originators (i.e. by department, function, division, section) so that documents may not be visible to disparate workgroups.
 - Originators monitor the progress and status of transactions they and/or their workgroups have initiated.
- k. Describe if the solution facilitates digital signing of documents via a computer web browser with modern browsers. Specify minimum software versions supported.
- l. Describe if the solution facilitates digital signing of documents on IOS, Android, and Windows smart phones. Specify minimum software versions supported.
- m. Also include whether the solution facilitates digital signing of documents on IOS, Android, and Windows mobile tablet devices. Specify minimum software versions supported.
- n. Address if the solution can create and manage multiple levels of system access.
- o. Describe if the solution will provide a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that: (1) the electronic document was not altered without detection during transmission or at any time after receipt; (2) any alterations to the electronic document during transmission or after receipt are fully documented.
- p. Clarify that the solution disallows any form of unauthorized copying or pasting signatures.
- q. Describe if the solution will determine if any modifications were made after the signature for the relevant sections were attached and disallow modifications or invalidate corresponding section that was modified.
- r. Explain if the solution will contain the copy of record, which will include
 - All electronic signatures contained in or logically associated with that document.
 - The date and time of receipt.
 - Any other information used to record the meaning of the document or the circumstances of its receipt.
 - Other, such as authorized system ID of signature owner, authorized computer ID, smart device ID such as MAC address, location data, etc.

- Detection of unauthorized data modification and place obvious marker on the document – electronic version and paper version.
- A function to alert users of needed actions.

2. Product Strategy Roadmap

The state needs a fully-developed plan Provide a 12-month Vendor product strategy as it relates to the solution proposed.

3. Disaster Recovery and Hosting Facilities

The state needs to understand the hosting facilities, capabilities and disaster recovery capabilities of the proposed solution, and requires an application disaster recovery plan as well. In addition to these needs, please address the following:

- Explain how the vendor will work with the state to develop this plan and integrate it with agency operation.
- The data that is stored in this application's database may be confidential and if so, must follow HIPAA, FERPA, PII and PCI compliance. Explain how the vendor will protect this data in the case of an event that requires execution of the disaster recovery plan.
- Describe the hosting facilities. Use diagrams where appropriate. Consider the following aspects:
 - Who is the hosting provider? Where is the primary site? Where is the disaster recovery site?
 - Explain if the hosting facilities are SAS 70 II compliant and/or compliant with SSAE 16 reporting standards, please provide copies of the most recent audit(s).
 - What is the data center's classification (Tier 1, Tier 2 etc.)?
 - What policies are in place to thwart insider breaches?
 - What is the process for background checks? Who are they performed by, for which employees, are the checks performed at employment, yearly, etc.
 - Will all customer data be housed within the continental United States?
 - Are there any circumstances when the solution would store customer data and intellectual property outside of the United States or with a non-USA owned institute?

4. Data Management

- Describe how data is archived and/or purged.
- The State must receive an attestation letter explaining how the Vendor destroyed the data when the State separates

from the Vendor. Please acknowledge that the solution will supply such communication.

- c. Describe how the state will get its data back in a form that can be used. What costs will be involved if any?
- d. How is the data destroyed at the end of a term contract?
 - Address how workflows, meta-data and configurations will be transferred to the state.

5. Audit

The state retains the right to audit the physical environment (could apply to production, secondary site, etc.) where the vendor application/service is hosted per the vendor proposal. Therefore, describe what processes the solution has in place to allow this audit?

- a. Describe if the solution will provide a retrievable audit trail.
- b. Supply the chain of custody for obtaining the record of copy.
- c. Address if the solution can export capabilities for the audit trail data. List possible export formats.
- d. Describe if audit event details are available to customer in a reusable format (i.e. CSV, Excel, PDF).
- e. Describe how the Audit trail is stored and secured against tampering.
- f. The solution must track every event in the signature process. Therefore, describe to what degree such details and events are being stored.
- g. Explain how consent from users to use the service is tracked as an auditable action.

6. NCID

For Identity Management, the state has invested in a common solution called NCID. NCID is the State's enterprise identity management (IDM) service and is operated by the North Carolina Office of Information Technology Services. (The details of NCID can be found at: <https://it.nc.gov/ncid/>.) Additional information regarding this service can be found in the ITS Service Catalog at: <http://www.its.state.nc.us/ServiceCatalog/Index.asp> (see Identity Management - NC Identity Management under the main menu item Application Services).

In consideration of this environment, describe the solution's capabilities to integrate with NCID. Also, explain the solution's capability to externalize NCID. Within **Section IV. Cost Proposal**, include an estimate to integrate NCID with the proposed solution understanding that this is a decentralized solution and will be invoiced by the individual agencies.

Please also address the following:

- a. Describe how the solution handles varying roles for authorization. Such as guest account (citizen non-authenticated), administrators, etc.
- b. The state seeks to achieve reduced or simplified sign-on capabilities. Describe how the solution supports reduced or simplified sign-on.
- c. It is possible that there will exist multiple identity stores or vaults. Explain the solution's capacity to handle federated identity.

7. Architecture

The state prefers a cloud-based, software as a service (SaaS) solution; therefore, please address the following:

- a. What is the solution's SaaS architecture model?
- b. Provide examples of scalability for very large organizations and numbers of concurrent and daily transactions.
- c. Describe how the application performs under load, both in terms of number the number of users and the transaction volume.
- d. Does the application dynamically scale based on runtime usage and demand?
- e. Provide details to further demonstrate that the proposed architecture and supported platform will scale to meet State current peak and future application processing and user demand.
- f. Describe the proposed solution's applications architecture, including offline capabilities, multi-language support, and interface standard supported.
- g. Describe the solution as related to smart devices and operations on smart devices including but not limited to smart pads, smart phones on various platforms. Include limitations in functionality, security, need for installation of facilitating software (apps) and possible additional costs.

8. Interoperability and Integration

The proposed solution may be required to interface with a variety of other systems. In consideration of this need, respond to the following:

- a. Please describe in detail what type of integration the solution supports; i.e., the integration architecture.
- b. Solution provides Application Programming Interfaces (APIs) for integration with other Customer systems. Include any details on Application Programming Interfaces (APIs) provided. Some of the potential integrations are:
 - SAP (SAP SSO cookies for example)
 - Web services (MQ Series, other APIs)
 - Enterprise Service Bus (e.g. Web Sphere Service Broker)
 - LDAP (for authentication)
 - NCID (for identity management)

- Document management systems (list)
 - Office software packages (Office 365)
 - Business systems such as human resources, accounting, finance, CRM, ERP, LMS, etc.
 - SharePoint Online and On Premises
 - Dynamics 365, Salesforce.com
- c. Are APIs secure and encrypted? What Encryption Method,
 - d. How do you extract form or record data? Do you use industry standards such as XML?
 - e. How is data inserted into a form? Can data be inserted dynamically (based on user inserted data)?
 - f. Can forms be processed via API in both real time and/or batch mode?
 - g. How does the API deal with multiple accounts (for enterprise-wide forms)?
 - h. Can the API retrieve software version numbers?
 - i. How are fields identified in the API?
 - j. How is the workflow engine capable of easily supporting a variety of e-forms?
 - k. The state prefers REST web service interfaces. XML schemas should be derived from industry standard vocabularies where possible such as the National Information Exchange Model (NIEM). Describe how the solution will support these and other interoperability standards.

9. Applications Management and Control

Describe the process of raising and managing exceptions within the application. Please include the following:

- a. Address whether multifactor authentication (MFA) access is available for all accounts including signatories, admins, and form builders? Is it included in the price? If not provide pricing in the cost section.
- b. Describe the level of customer control on the timing of applying patches, upgrades, and changes to the SaaS application and the notification process to be used.
- c. Explain the process for handling software defects.
- d. Describe the major and minor release policy for the solution.
- e. Describe user configuration capabilities.
- f. Describe user self-provisioning capabilities.
- g. Describe the level and skill set needed by the State to administer and configure the proposed solution.
- h. How do you address Delegation of authority?
- i. Describe how privileged management accounts are secured, provide encrypted authentication and access to authorized users.

- j. Specifically, does the Delegation of Authority capability that allows signatories to delegate signing authority for documents for a specified period of time, or indefinitely.

10. Application Specifications

Please describe how the solution will include the following application specifications:

- a. Describe integration with Microsoft Office 365 Office Productivity & Email.
- b. Describe how the solution can initiate the signature process with PDF and Word documents. *Please note that the vendor may apply custom branding (official logos, colors, hyperlinks) as necessary to create a consistent user experience. Please see **Section III, #6** for more information.*
- c. Describe how the solution works with Section 508 compliant screen readers and other ADA capabilities. Specifically, in-process and completed documents should be fully read by a screen reader.
- d. Provides a digital signature solution in which the "root" digital certificate is provided by a certificate authority that meets assurance and trust requirements by Adobe. Documents with these certificates become automatically trusted by Adobe as this facilitates the ability to validate the signature. More information about Adobe's Approved Trust List and current members of that list can be found at <http://helpx.adobe.com/acrobat/kb/approved-trust-list2.html>.
- e. Provides the ability for anyone to open a digitally signed PDF and observe a signature validity confirmation across the top of the file that indicates all signatures are signed and valid.
- f. Users of the e-signature service are given an opportunity to decline to use the service.
- g. Does the solution provide the capability for electronic notarization.
- h. Digital signature notifications are achievable through SMTP relay, direct email client integration (i.e. "mailto:"), or SMS (text messages). Please describe these and/or other capabilities.
- i. Describe what notifications are sent to a user for signature?
- j. Please describe the solution's policy for handling customer's intellectual property, data, and information.
- k. Describe if the solution can import a predefined electronic list (i.e. CSV, ODBC, Excel) of customer's vendors and business partners. Please describe capability and any limitations that may exist.

11. Automation of Forms

Explain how the solution will address the automation of forms.
Provide an explanation regarding the:

- a. Process for integrating field validation (both data and format).
- b. Process for database integration.
- c. The limitations on the number of standard templates that can exist.
- d. Level at which standard templates exist – whole org., division, etc? Provide examples.
- e. Revision process to forms without customization from vendor.
- f. Use of existing form templates created by other products.
- g. Methodology regarding how calculations are conducted within form.
- h. Process for creating and publishing forms to agency websites.
- i. Process required for citizens to use forms posted to Agency websites via the solution.
- j. Methodology regarding how persons in a workflow can redline data in a form that is in process and route that form back to the originator for revision. Describe the form data capture – stored in form replica and/or recreated from database and ability to extract either way.
- k. Process for pre-populating user-specific information such as name, address, and etc.
- l. Solution's method for marking sections of the document where signature is required.
- m. Solution will allow forms to be labeled by type of process, such as HR, Finance, Payroll, etc.

12. Workflow

Describe the solution's workflow capabilities. Include the functionalities below within the description:

- a. Provide examples of templates for developing workflows per the solution that will standardize business engineering processes and improve workflow development efficiency.
- b. Any limitations to the size of documents sent through workflow.
- c. Any limitations to the combined file size of a transaction with multiple files attached.
- d. Each person in the workflow is given the opportunity to review all documents, with a confirmation opportunity, before the transaction continues.
- e. The solution allows for rejection. If a form is rejected, specify how commenting, rerouting, markup of document is allowed.
- f. The solution supports the approving/rejecting of multiple sections of a document by more than one approver and/or signer.
- g. Workflows are setup based on Roles and Permissions

- h. User initiates signing.
- i. Each department/division/unit can have and maintain their own customizable workflows.
- j. Routing of multiple types of documents with multiple signatures within a single transaction.
- k. Users can track the progress of a transaction – including stage and status.
- l. The process for copying previously created workflows
- m. The solution generates a diagram of the workflow.
- n. User can abandon signing a document.
- o. Portions of the workflow that are configurable by the Department/Division/Unit.
- p. Queues are established to assist users to process, review, analyze and approve depending on role.
- q. Support Ad Hoc signing from cloud and smart devices.
- r. Workflow creation can be automated, (i.e. – Roles copied from other systems such as HR/Payroll systems).
- s. Documents which do not require signature are bound to signature documents and routed through the workflow.
- t. Workflow can be redirected and users injected to the flow.
- u. Support branding and color scheme customization of document packages for signature.
- v. Support document creator workflow rerouting with and without workflow start over.
- w. How an external system process can be added as a workflow step/approval.
- x. Describe how the solution will generate workflow and forms meta-data and the content of such meta-data specifying what is included, and what is excluded.

13. Signature/Initialing

Describe the solution's signature and initialing capabilities. Include how the:

- a. Digital signature is linked to the documents being signed. Describe how this is achieved.
- b. Solution assigns and restricts the sole control of the signature to the owner.
- c. Solution captures the users "actual" signature and initials.
- d. Solution captures a picture of the signature owner and associates it with the actual signature.
- e. Solution captures speed, pressure and x-y coordinates of signatures.
- f. Receiver of data can determine origin.
- g. Electronic document cannot be altered without detection at any time after being signed.
- h. Code or other mechanism is used to create digital signatures and how that code or mechanism is unique to that individual at the time of signature.

14. Repudiation

Describe how the solution addresses repudiation; specifically address how the solution will provide:

- a. True and correct copy of document received – provide sufficient evidence to show how the copy of record was derived from and accurately reflects the electronic document as it was received by the system, this evidence is also necessary to establish document integrity.
- b. A human-readable format that clearly and accurately associates all the information provided in electronic document with descriptions or labeling of the information and provides the opportunity to repudiate the electronic document based on this review.
- c. Inclusion of other information necessary to record meaning of document – such as data field labels, signatory information such as references to validation mechanism, and transmission source information.
- d. Procedures to address submitter/signatory repudiation of a copy of record.
- e. Confirmation of receipt of intact form data or record.
- f. Expunging of transaction upon authorized request.
- g. Long term validation of electronically signed document. Describe how electronically signed document will maintain validity for long term (multiple years out).

15. Notification

Describe the solution's notification capabilities, include if the solution:

- a. Provides opportunity to review certification statements and warnings (including any applicable certifications that false certification carries criminal penalties).
- b. Provides notification that copy of record is available and this notification is configurable by each Department/Division/Unit.
- c. Flags accidental submissions.
- d. Supports setting expirations and notifications.
- e. Has expirations and notifications that can be set for a standard (e.g. three-month expiry) for whole organization, a division, and individual and etc.
- f. Makes it clear that the signed document represents a completed declaration of will, and not just a draft which the signatory did not intend to be bound by – Finality function.
- g. Makes a signatory aware that by his/her signature he/she is entering into a binding transaction – Cautionary function.
- h. Includes automatic acknowledgement of receipt.

16. Storage

Describe the following storage capabilities; include if the solutions storage functionality can:

- a. To print or store locally by person(s) in the process.
- b. Form data or record will be stored – vendor or agency.
- c. Provide costs estimate for vendor storage in **Section IV**. Provide cost estimate for any transmission cost if stored at agency in **Section IV**.
- d. Store and accommodate according to each department/division/unit record retention and disposition schedule.
- e. Allow procedures for retrieving documents from Vendor; during contract term.
- f. Allow procedures for retrieving documents from Vendor; expired contract term.
- g. Format documents are received and stored in.
- h. Support document package labeling for ease of segmented document storage outside of the native solution data center
- i. Process for retrieving information required to meet eDiscovery requests when documents are stored at a Vendor operated or controlled site; or when information retrieval requires participation of the Vendor or a third party.
- j. Process for searching and sorting information stored at Agency site to meet eDiscovery requests (e.g. – record identifiers).
- k. Exit Strategy –Define how this process would work and what costs would be involved. Is there a cost for transferred data?

17. Service Level Agreement (SLA) and Reporting

The ideal solution will have a detailed Service Level Agreement (SLA)

- a. Provide a copy of the proposed Service Level Agreement (SLA). Including notation of optional levels of service and Breaches in SLA from a Financial standpoint.
- b. What is the standard service availability that the solution commits to provide in a Service Level Agreement (SLA)? Please provide quantitative response in percentage (%) and any other details to describe this service availability commitment.
- c. Is the SLA Financially backed?
- d. With respect to RPO and RTO, please describe how the solution provided allows for an RPO of 24 hours and an RTO of 24-48 hours. Describe the architectural approach, infrastructure and operating environment that are necessary to meet the stated recovery point and time objectives. In addition, tell us if the proposed solution exceeds those metrics.
- e. Describe report and metrics generation capabilities. Show examples of how utilization can be tracked by user or groups of users.

- f. The state will require a rolled-up view of all usage broken down by agency quarterly and yearly; therefore, describe how the solution will allow agencies to run their own usage reports.
- g. The total transaction volume can be tracked by month, by Department/Division/Unit, and reported to DIT.

18. Software Support and Maintenance Services

The ideal solution will have established support and maintenance. Please explain the following regarding these services:

- a. Describe how the service desk operates; i.e., service hours, escalation of problems, ticket tracking, reporting of metrics on availability, call scripts, repository of solutions, call back time etc.
- b. Describe how the solution will provide availability and uptime metrics for solution.
- c. Describe the solution's development "sandbox" as envisioned for backend integration efforts with legacy environments.
- d. Describe how the application changes will be able to be previewed in a "sandbox"/non-production environment prior to changes being made in production.
- e. Describe the management and project team assigned to work with North Carolina.
- f. Describe the process for incident management, change management and release management.
- g. Provide a list and description of the required roles and level of staff resources to manage, monitor, maintain and support the overall solution.

19. Training

The State desires a solution that will employ training techniques with the capability to accommodate various levels of users. Training will be needed for each department/division/unit to include form modification, workflow creation/modifications, and assistance with onboarding users including signature creation. Describe the solution's training regarding:

- a. What modes of user training are available?
- b. What level of training comes with the proposal?
- c. What type of training will be provided in the proposal for the new use cases and purchases? (to include form modification, workflow creation/modifications, and assistance with on-boarding users including signature creation.)
- d. What online help capabilities are available for users?
- e. What online help capabilities are available for administrators?
- f. What web-based documentation is provided?

- g. What live and web-based technical support is provided?
- h. What types of training and documentation is provided for API usage?
- i. Describe the ability to provide cloud based user "sandbox" areas to support user on boarding, training, and functional trials. Specifically discuss limitations as related to function of the production system as well as trial or usage limits.
- j. Describe whether the proposed solution requires customer to procure or implement any additional, on-premise hardware or technology commodities for proposed solution to function. Specify requirements by including descriptions, manufacturers, and model numbers.
- k. Provide information regarding user communities and/or support groups.

IV. Cost Proposal

OFFER COSTS: The Vendor must list and describe any applicable offer costs which may include the following:

- 1) Vendor shall be able to accept individual and/or Agency Wide Purchases on behalf of the agency and count toward the tiered pricing of that Agency.
- 2) Can Transactions/licensing fees be billed by Department/Division/Unit?
- 3) Pricing based on total transaction volume for the State.
- 4) Explain usage and meaning of document, folder, and transaction system identifiers. Usage counts will need to correspond with Cost Proposal in **Section IV**.
- 5) Describe the purchase process for an Agency.
- 6) Define the minimum transaction purchase.
- 7) Define the Costs for Connectors to *SharePoint, Dynamics 365, Salesforce etc.*
 - a. What costs are there to integrate into SharePoint?, Azure, Amazon Webservices, Dynamics 365, and Salesforce.com.
 - b. What other CRM solutions or cloud solutions do you integrate with? Provide list and a cost for each.
- 8) Define what is included in the Named users, Tiered, and unlimited pricing models. Support, training, adoption etc..
- 9) Define Unlimited or Enterprise in terms of who can utilize this model.
- 10) Define what constitutes a transaction from a cost standpoint? Specifically, Voided Transactions and bulk Downloads.
- 11) Define Adoption accelerator costs if offered?
- 12) Define the service level, description and costs for Standard, Premium, and Dedicated Support?
- 13) Is Unlimited phone technical support available for users, power users and administrators?
- 14) Define what happens to the number of Transactions that are not used during the contract term and yearly anniversary.
- 15) Define the licensing model offered and how signatures and transactions are counted.

- 16) NCID Integration-This is a de-centralized model and each Agency will have its own solution; therefore, define the cost for integration. Consider
- Storage – How much storage is included with each cost model.
 - Exit Strategy – Define the cost for downloading transactions- Define how this process works
 - What is the cost for bulk retrieval of documents?
 - Migration costs from existing signature systems
 - Are there costs for Voided Transaction if any?
 - Is there customization required or proposed addressing specification; If so, what is the cost.
 - Are there additional modules required or proposed addressing specifications
 - Are there any installation/conversion/integration/transition costs?
 - Provide all training costs by type; user, admin, power user. What is included in each cost model.
 - Maintenance costs per year- Is this an evergreen product and updates are included?
 - Do you have a professional consulting service or other value added service based on hourly rates? Provide your hourly costs. Travel and lodging expenses, if any, must be thoroughly described; and are limited by the State's Terms and Conditions.

Item #	QTY	Unit	Description	Ext Cost
1.	1	User/year	Named User	
2.	5	Users/year	Named User	
3.	25	Users/year	Named User	
4.	100	Transaction/year	Package of signatures	
5.	500	Transaction/year	Package of signatures	
6.	2500	Transaction/year	Package of signatures	
7.	5000	Transaction/year	Package of signatures	
8.	10000	Transaction/year	Package of signatures	
9.	20000	Transaction/year	Package of signatures	
10.	50000	Transaction/year	Package of signatures	

Item #	QTY	Unit	Description	Ext Cost
11.	75000	Transaction/year	Package of signatures	
12.	100000	Transaction/year	Package of signatures	
13.	Unlimited	Transaction/year	Package of signatures	
14.	NA	NA	NCID integration	
15.	Storage	MB	Cost for Form Storage	
16.		Per Connector	Connector to Dynamics 365	
17.		Per Connector	Connector to Salesforce	
18.		Per Connector	Connector to SharePoint Online	
19.		Per Connector	Connector to SharePoint On Prem	
20.			Bulk retrieval of Transactions	
21.		Per hour?	Migration Costs	
22.	Vendor Define	Transaction/year	Costs for Voided Transactions	
23.	Vendor Define	Per hour	Professional Services	

17) PAYMENT PLAN PROPOSAL:

Vendors should note that multiple State agencies will leverage this contract, subsequently requiring the awarded vendor to invoice and provision each individual agency separately.

If Buying licenses/transactions in the middle of the term then they should be co-termed and prorated to the contract anniversary date.

- 18) **ALTERNATIVE COST RESPONSE**: Vendors who propose an Alternative cost response must submit a separate document labeled "ALTERNATIVE COST RESPONSE".

V. Other Requirements and Special Terms

- 1) **VENDOR UTILIZATION OF WORKERS OUTSIDE U.S.:** In accordance with N.C.G.S. §143B-1361(b), the Vendor must detail the manner in which it intends to utilize resources or workers in the RFP response. The State of North Carolina will evaluate the additional risks, costs, and other factors associated with such utilization prior to making an award for any such Vendor's offer. The Vendor shall provide the following for any offer or actual utilization or contract performance:
 - a) The location of work performed under a state contract by the Vendor, any subcontractors, employees, or other persons performing the Agreement and whether any of this work will be performed outside the United States
 - b) The corporate structure and location of corporate employees and activities of the Vendors, its affiliates or any other subcontractors
 - c) Notice of the relocation of the Vendor, employees of the Vendor, subcontractors of the Vendor, or other persons performing Services under a state contract outside of the United States
 - d) Any Vendor or subcontractor providing call or contact center Services to the State of North Carolina shall disclose to inbound callers the location from which the call or contact center Services are being provided

Will any work under the Agreement be performed outside the United States?

Where will Services be performed:

YES _____ NO _____

2) SPECIAL TERMS AND CONDITIONS:

- a) Paragraph #19 of the DIT Terms and Conditions is supplemented as follows: Any such audit shall be conducted only upon prior written notice of 30 days or more, and with the concurrence of The State for the date and time of any audit, and adherence to The State's security requirements during regular business hours at The State's offices and shall not unreasonably interfere with The State's business activities.
 - b) Paragraph #16 of the DIT Terms and Conditions is supplemented as follows: Each agency will be in their own instance and can successfully build and release signature transactions.
 - c) Reserved
 - d) Maintenance
- 3) **FINANCIAL STATEMENTS:** The Vendor shall provide evidence of financial stability with its response to this RFP as further described hereinbelow. As used herein, Financial Statements shall exclude tax returns and compiled statements.
- a) For a publicly traded company, Financial Statements for the past three (3) fiscal years, including at a minimum, income statements, balance sheets, and statement of changes in financial position or cash flows. If three (3) years of financial statements are not available, this information shall be provided to the fullest extent possible, but not less than one year. If less than 3 years, the Vendor must explain the reason why they are not available.

- b) For a privately held company, when certified audited financial statements are not prepared: a written statement from the company's certified public accountant stating the financial condition, debt-to-asset ratio for the past three (3) years and any pending actions that may affect the company's financial condition.
 - c) The State may, in its sole discretion, accept evidence of financial stability other than Financial Statements for the purpose of evaluating Vendors' responses to this RFP. The State reserves the right to determine whether the substitute information meets the requirements for Financial Information sufficiently to allow the State to evaluate the sufficiency of financial resources and the ability of the business to sustain performance of this RFP award. Scope Statements issued may require the submission of Financial Statements and specify the number of years to be provided, the information to be provided, and the most recent date required.
- 4) **DISCLOSURE OF LITIGATION:** Reserved.
 - 5) **CRIMINAL CONVICTION:** Reserved.
 - 6) **SECURITY AND BACKGROUND CHECKS:** Reserved.
 - 7) **ASSURANCES:** Reserved.
 - 8) **CONFIDENTIALITY OF DATA AND INFORMATION:** All RFP responses, information marked as confidential or proprietary, financial, statistical, personnel, technical and other data and information relating to the State's operation which are designated confidential by the State and made available to the Vendor in order to carry out the Agreement or which become available to the Vendor in carrying out the Agreement, shall be protected by the Vendor from unauthorized use and disclosure through the observance of the same or more effective procedural requirements as are applicable to the State. If the methods and procedures employed by the Vendor for the protection of the Vendor's data and information are deemed by the State to be adequate for the protection of the State's confidential information, such methods and procedures may be used, with the written consent of the State, to carry out the intent of this section. The Vendor shall not be required under the provisions of this section to keep confidential, (1) information generally available to the public, (2) information released by the State generally, or to the Vendor without restriction, (3) information independently developed or acquired by the Vendor or its personnel without reliance in any way on otherwise protected information of the State. Notwithstanding the foregoing restrictions, the Vendor and its personnel may use and disclose any information which it is otherwise required by law to disclose, but in each case only after the State has been so notified, and has had the opportunity, if possible, to obtain reasonable protection for such information in connection with such disclosure.
 - 9) **SOFTWARE TERMS:** Reserved.
 - 10) **PROJECT MANAGEMENT:** All coordination on behalf of the Agency shall be through a single point of contact designated as the Agency Project Manager. Vendor shall designate a Vendor Project Manager who will provide a single point of contact for management and coordination of Vendor's work. All work

performed pursuant to the Agreement shall be coordinated between the Agency Project Manager and the Vendor's Project Manager.

- 11) **MEETINGS:** The Vendor is required to meet with Agency personnel, or designated representatives, to resolve technical or contractual problems that may occur during the term of the Agreement. Meetings will occur as problems arise and will be coordinated by Agency. The Vendor will be given reasonable and sufficient notice of meeting dates, times, and locations. Conference calls are should be sufficient as opposed to face-to-face meeting. Consistent failure to participate in problem resolution meetings, two (2) consecutive missed or rescheduled meetings, or failure to make a good faith effort to resolve problems, may result in termination of the Agreement.
- 12) **STOP WORK ORDER:** The State may issue a written Stop Work Order to Vendor for cause at any time requiring Vendor to suspend or stop all, or any part, of the performance due under the Agreement for a period up to ninety (90) days after the Stop Work Order is delivered to the Vendor. The ninety (90) day period may be extended for any further period for which the parties may agree.
 - a) The Stop Work Order shall be specifically identified as such and shall indicate that it is issued under this term. Upon receipt of the Stop Work Order, the Vendor shall immediately comply with its terms and take all reasonable steps to minimize incurring costs allocable to the work covered by the Stop Work Order during the period of work suspension or stoppage. Within a period of ninety (90) days after a Stop Work Order is delivered to Vendor, or within any extension of that period to which the parties agree, the State shall either:
 - i) Cancel the Stop Work Order, or
 - ii) Terminate the work covered by the Stop Work Order as provided for in the termination for default or the termination for convenience clause of the Agreement.
 - b) If a Stop Work Order issued under this clause is canceled or the period of the Stop Work Order or any extension thereof expires, the Vendor shall resume work. The State shall make an equitable adjustment in the delivery schedule, the Agreement price, or both, and the Agreement shall be modified, in writing, accordingly, if:
 - i) The Stop Work Order results in an increase in the time required for, or in the Vendor's cost properly allocable to the performance of any part of the Agreement, and
 - ii) The Vendor asserts its right to an equitable adjustment within thirty (30) days after the end of the period of work stoppage; provided that if the State decides the facts justify the action, the State may receive and act upon an offer submitted at any time before final payment under the Agreement.
 - c) If a Stop Work Order is not canceled and the work covered by the Stop Work Order is terminated in accordance with the provision entitled Termination for Convenience of the State, the State shall allow reasonable

direct costs resulting from the Stop Work Order in arriving at the termination settlement.

The State shall not be liable to the Vendor for loss of profits because of a Stop Work Order issued under this term.

- 13) **TRANSITION ASSISTANCE:** If this Agreement is not renewed at the end of this term, or is canceled prior to its expiration, for any reason, the Vendor must provide for up to six (6) months after the expiration or cancellation of the Agreement all reasonable transition assistance requested by the State, to allow for the expired or canceled portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Services to the State or its designees. Such transition assistance will be deemed by the parties to be governed by the terms and conditions of the Agreement, (notwithstanding this expiration or cancellation) except for those Contract terms or conditions that do not reasonably apply to such transition assistance. The State shall pay the Vendor for any resources utilized in performing such transition assistance at the most current rates provided by the Agreement for Contract performance. If the State cancels the Agreement for cause, then the State will be entitled to offset the cost of paying the Vendor for the additional resources the Vendor utilized in providing transition assistance with any damages the State may have otherwise accrued as a result of said cancellation.
- 14) **TERM EXTENSIONS:** This agreement allows month-to-month or other term extensions at the discretion of the State.
- 15) **FINANCIAL RESOURCES ASSESSMENT, QUALITY ASSURANCE, PERFORMANCE AND RELIABILITY:**
 - a) Pursuant to N.C.G.S. §143B-1350(h)(1), Agencies must conduct a risk assessment, including whether the Vendor's has sufficient financial resources to satisfy the agreed upon limitation of liability prior to the award of a contract with Vendor.
 - b) Contract Performance Security. The State reserves the right to require performance guaranties pursuant to N.C.G.S. §143B-1340(f) and 09 NCAC 06B.1207 from the Vendor without expense to the State.
 - c) Project Assurance, Performance and Reliability Evaluation – Pursuant to N.C.G.S. §143B-1340, the State CIO may require quality assurance reviews of Projects as necessary.
- 16) **UNANTICIPATED TASKS:** Reserved.
- 17) **DUE DILIGENCE:** Reserved.
- 18) **AGENCY SITE VISITS:** Reserved.
- 19) **VENDOR SITE VISITS:** Reserved.
- 20) **RESELLERS:** If the Offer is made by a Reseller that purchased the offered items for resale or license to the Agency, or offered based upon an agreement between the Offeror and a third party, and that the proprietary and intellectual property rights associated with the items are owned by parties other than the Reseller ("Third Parties"). The Agency further acknowledges that except for the payment to the Reseller for the Third Party items, all of its rights and

obligations with respect thereto flow from and to the Third Parties. The Reseller shall provide the Agency with copies of all documentation and warranties for the Third Party items which are provided to the Reseller. The Reseller shall assign all applicable third party warranties for Deliverables to the Agency. The State reserves all rights to utilize existing agreements with such Third Parties or to negotiate agreements with such Third Parties as the State deems necessary or proper to achieve the intent of this RFP..

VI. Proposal Content and Organization

- 1) **CONTENTS OF PROPOSAL**: This section should contain all relevant and material information relating to the Vendor's organization, personnel, and experience that would substantiate its qualifications and capabilities to perform the Services and/or provide the goods described in this RFP. If any relevant and material information is not provided, the offer may be rejected from consideration and evaluation. Offers will be considered and evaluated based upon the Vendor's full completion and response to the following, and any additional requirements herein, or stated in a separate Exhibit.
- 2) **INFORMATION AND DESCRIPTIVE LITERATURE**: The Vendor must furnish all information requested; and if response spaces are provided in this document, the Vendor shall furnish said information in the spaces provided. Further, if required elsewhere in this RFP, each Vendor must submit with their offer sketches, descriptive literature and/or complete specifications covering the products offered. References to literature submitted with a previous offer will not satisfy this provision. Proposals that do not comply with these requirements may be rejected.
- 3) **PROPOSAL CONTENT**: Demonstrate substantial conformity to the RFP specifications.
 - a) Clearly state the understanding of the problem(s) presented by this RFP.
 - i) Response to technical specifications
 - ii) Cost offer
 - b) Detailed description of Vendor's firm should include all of the following:
 - i) Full name, address, and telephone number of the organization;
 - ii) Date established;
 - iii) Background of firm;
 - iv) Ownership (public company, partnership, subsidiary, etc.);
 - v) If incorporated, state of incorporation must be included.
 - vi) Number of full-time employees on January 1st for the last three years or for the duration that the Vendor's firm has been in business, whichever is less.
- 4) **ERRATA OR EXCEPTIONS**: Any errata or exceptions must be stated on a separate page, labeled "Errata and/or Exceptions" with references to the corresponding terms or provisions of the Solicitation.

- 5) **OFFER FORMAT:** The offers should contain the entire solicitation and be organized in the exact order in which the requirements and/or desirable performance criteria are presented in the RFP. **The Execution page of this RFP must be placed at the front of the Proposal.** Each page should be numbered. The offer should contain a table of contents, which cross-references the RFP requirement and the specific page of the response in the Vendor's offer. All offers should be typewritten on standard 8 1/2 x 11 paper (larger paper is permissible for charts, spreadsheets, etc.) and placed within a binder with tabs delineating each section.
- 6) **GENERAL INSTRUCTIONS:** Vendors are strongly encouraged to adhere to the following general instructions in order to bring clarity and order to the offer and subsequent evaluation process:
 - a) Elaborate offers in the form of brochures or other presentations beyond that necessary to present a complete and effective offer are not desired.
 - b) The response should be complete and comprehensive with a corresponding emphasis on being concise and clear.
- 7) **RFP RESPONSE ORGANIZATION:** The offer should be organized and indexed in the following format and should contain, at a minimum, all listed items in the sequence indicated.
 - a) Letter of Transmittal - Each offer must be accompanied by a letter of transmittal that provides the following information:
 - i) Identify the submitting organization;
 - ii) Identify the name, title, telephone and fax number, along with an e-mail address of the person authorized by the organization to contractually obligate the organization;
 - iii) Identify the name, title, telephone and fax number, along with an e-mail address of the person authorized to negotiate the Agreement on behalf of the organization;
 - iv) Identify the names, titles, telephone and fax number, along with an e-mail address of the person to be contacted for clarification;
 - v) Acknowledge receipt of any and all amendments to this RFP.
 - b) Table of Contents.
 - c) Response to Technical Specifications.
 - d) Completed Cost Offer.
 - e) References.
 - f) Financial Information.
 - g) Conflict of Interest:
 - i) Provide a statement that no assistance in preparing the response was received from any current or former employee of the State of North Carolina whose duties relate(d) to this RFP, unless such assistance was provided by the state employee in his or her official public capacity and that neither such employee nor any member of his or her immediate family has any financial interest in the outcome of this RFP;

- ii) State if the Vendor or any employee of the Vendor is related by blood or marriage to an Agency employee or resides with an Agency employee. If there are such relationships, list the names and relationships of said parties. Include the position and responsibilities within the Vendor's organization of such Vendor employees; and
 - iii) State the employing State Agency, individual's title at that State Agency, and termination date.
 - h) Errata and Exceptions, if any. Offers conditioned upon acceptance of Vendor Exceptions may be determined to be non-responsive by the State.
 - i) Copy of the Vendor's License and Maintenance Agreements, if any. The State reserves the right to edit or modify these agreements to conform to the best interest of the State.
 - j) Other Supporting Material Including Technical System Documentation.
 - k) Training and Other Materials, Samples or Examples.
 - l) Within each section of their offer, Vendors should address the items in the order in which they appear in this RFP. Forms, if any provided in the RFP, must be completed and included in the appropriate section of the offer. All discussion of proposed costs, rates, or expenses must be presented with the cost response.
- 8) **ADHERENCE TO INSTRUCTIONS:** Any offer that does not adhere to these instructions may be deemed non-responsive and rejected on that basis.
- 9) **ATTACHMENTS:** Vendors may attach other materials that they feel may improve the quality of their responses. However, these materials should be included as items in a separate appendix.

Attachment A. Department of Information Technology Terms and Conditions

1) DEFINITIONS:

- a) "Data" includes means information, formulae, algorithms, or other content that the State, the State's employees, agents and end users upload, create or modify using the Services pursuant to this Agreement. Data also includes user identification information and metadata which may contain Data or from which the State's Data may be ascertainable.
- b) **Deliverable/Product Warranties** shall mean and include the warranties provided for products or deliverables licensed to the State as included in Paragraph 7) c) of these Terms and Conditions unless superseded by a Vendor's Warranties pursuant to Vendor's License or Support Agreements.
- c) "Services" shall mean the duties and tasks undertaken by the Vendor to fulfill the requirements and specifications of this solicitation, including, without limitation, providing web browser access by authorized users to certain Vendor online services identified herein, and to related services, such as Vendor hosted Computer storage, databases, Support, documentation, and other functionalities.
- d) "State" shall mean the State of North Carolina, the Department of Information Technology as an agency, or the agency identified in this solicitation as the Purchasing Agency and Award Authority.
- e) "Support" includes provision of ongoing updates and maintenance for the Vendor online software applications, and as may be specified herein, consulting, training and other support Services as provided by the Vendor for users receiving similar Services.

2) ACCESS AND USE OF ONLINE SERVICES:

- a) Vendor grants the State a personal non-transferable and non-exclusive right to use and access, all Services and other functionalities or services provided, furnished or accessible under this Agreement. The State may utilize the Services as agreed herein and in accordance with any mutually agreed Acceptable Use Policy. The State is authorized to access State Data and any Vendor-provided data as specified herein and to transmit revisions, updates, deletions, enhancements, or modifications to the State Data. This shall include the right of the State to, and access to, Support without the Vendor requiring a separate maintenance or support agreement. Subject to an agreed limitation on the number of users, the State may use the Services with any computer, computer system, server, or desktop workstation owned or utilized by the State or other authorized users. User access to the Services shall be routinely provided by the Vendor and may be subject to a more specific Service Level Agreement (SLA) agreed to in writing by the parties. The State shall notify the Vendor of any unauthorized use of any password or account, or any other known or suspected breach of security access. The State also agrees to refrain from taking any steps, such as reverse engineering, reverse assembly or reverse compilation to derive a source code equivalent to the Services or any portion thereof. Use of the Services to perform services for commercial third parties (so-called "service bureau" uses) is not permitted, but the State may utilize the Services to perform its governmental functions. If the Services fees are based upon the number of Users and/or hosted instances, the number of Users/hosted instances available may be adjusted at any time (subject to the restrictions on the maximum number of Users specified in the Furnish and Deliver Table herein above) by mutual agreement and State Procurement approval. All Services and information designated as "confidential" or "proprietary" shall be kept in confidence except as may be required by the North Carolina Public Records Act: N.C.G.S. § 132-1, *et. seq.*
- b) The State's right to access the Services and its associated services neither transfers, vests, nor infers any title or other ownership right in any intellectual property rights of the Vendor or any third party, nor does this right of access transfer, vest, or infer any title or other ownership right in any source code associated with the Services unless otherwise agreed to by the parties. The provisions of this paragraph will not be construed as a sale of any ownership rights in the Services. Any Services or technical and business information owned by Vendor or its suppliers or licensors made accessible or furnished to the State

shall be and remain the property of the Vendor or such other party, respectively. Vendor has a limited, non-exclusive license to access and use the State Data as provided to Vendor, but solely for performing its obligations under this Agreement and in confidence as provided herein.

- c) Vendor or its suppliers shall at minimum, and except as otherwise agreed, provide telephone assistance to the State for all Services procured hereunder during the State's normal business hours (unless different hours are specified herein). Vendor warrants that its Support and customer service and assistance will be performed in accordance with generally accepted industry standards. The State has the right to receive the benefit of upgrades, updates, maintenance releases or other enhancements or modifications made generally available to Vendor's users for similar Services. Vendor's right to a new use agreement for new version releases of the Services shall not be abridged by the foregoing. Vendor may, at no additional charge, modify the Services to improve operation and reliability or to meet legal requirements.
 - d) Vendor will provide to the State the same Services for updating, maintaining and continuing optimal performance for the Services as provided to other similarly situated users or tenants of the Services, but minimally as provided for and specified herein. Unless otherwise agreed in writing, Support will also be provided for any other (e.g., third-party) software provided by the Vendor in connection with the Vendor's solution herein. The technical and professional activities required for establishing, managing, and maintaining the Services environment are the responsibilities of the Vendor. Any training specified herein will be provided by the Vendor to certain State users for the fees or costs as set forth herein or in an SLA.
 - e) Services provided pursuant to this Solicitation may, in some circumstances, be accompanied by a user clickwrap agreement. The term clickwrap agreement refers to an agreement that requires the end user to manifest his or her assent to terms and conditions by clicking an "ok" or "agree" button on a dialog box or pop-up window as part of the process of access to the Services. All terms and conditions of any clickwrap agreement provided with any Services solicited herein shall have no force and effect and shall be non-binding on the State, its employees, agents, and other authorized users of the Services.
 - f) The Vendor may utilize partners and/or subcontractors to assist in the provision of the Services, so long as the State Data is not removed from the United States unless the terms of storage of the State Data are clearly disclosed, the security provisions referenced herein can still be complied with, and such removal is done with the prior express written permission of the State. The Vendor shall identify all of its strategic business partners related to Services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.
 - g) Vendor warrants that all Services will be performed with professional care and skill, in a workmanlike manner and in accordance with the Services documentation and this Agreement.
 - h) An SLA or other agreed writing shall contain provisions for scalability of Services and any variation in fees or costs as a result of any such scaling.
 - i) Professional services provided by the Vendor at the request by the State in writing in addition to agreed Services shall be at the then-existing Vendor hourly rates when provided, unless otherwise agreed in writing by the parties.
- 3) **WARRANTY OF NON-INFRINGEMENT; REMEDIES.**
- a) Vendor warrants to the best of its knowledge that:
 - i) The Services do not infringe any intellectual property rights of any third party; and
 - ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party;
 - b) Should any Services supplied by Vendor become the subject of a claim of infringement of a patent, copyright, Trademark or a trade secret in the United States, the Vendor, shall at its option and expense, either procure for the State the right to continue using the Services, or replace or modify the same to become noninfringing. If neither of these options can

reasonably be taken in Vendor's judgment, or if further use shall be prevented by injunction, the Vendor agrees to cease provision of any affected Services, and refund any sums the State has paid Vendor and make every reasonable effort to assist the State in procuring substitute Services. If, in the sole opinion of the State, the cessation of use by the State of any such Services due to infringement issues makes the retention of other items acquired from the Vendor under this Agreement impractical, the State shall then have the option of terminating the Agreement, or applicable portions thereof, without penalty or termination charge; and Vendor agrees to refund any sums the State paid for unused Services.

- c) The Vendor, at its own expense, shall defend any action brought against the State to the extent that such action is based upon a claim that the Services supplied by the Vendor, their use or operation, infringes on a patent, copyright, trademark or violates a trade secret in the United States. The Vendor shall pay those costs and damages finally awarded or agreed in a settlement against the State in any such action. Such defense and payment shall be conditioned on the following:
 - i) That the Vendor shall be notified within a reasonable time in writing by the State of any such claim; and,
 - ii) That the Vendor shall have the sole control of the defense of any action on such claim and all negotiations for its settlement or compromise provided, however, that the State shall have the option to participate in such action at its own expense.
- d) Vendor will not be required to defend or indemnify the State if any claim by a third party against the State for infringement or misappropriation results from the State's material alteration of any Vendor-branded Services, or from the continued use of the good(s) or Services after receiving notice they infringe on a trade secret of a third party.

4) ACCESS AVAILABILITY; REMEDIES:

- a) The Vendor warrants that the Services will be in good working order, and operating in conformance with Vendor's standard specifications and functions as well as any other specifications agreed to by the parties in writing, and shall remain accessible 24/7, with the exception of scheduled outages for maintenance and of other service level provisions agreed in writing, e.g., in an SLA. Vendor does not warrant that the operation of the Services will be completely uninterrupted or error free, or that the Services functions will meet all the State's requirements, unless developed as Customized Services.
- b) The State shall notify the Vendor if the Services are not in good working order or inaccessible during the term of the Agreement. Vendor shall, at its option, either repair, replace or reperform any Services reported or discovered as not being in good working order and accessible during the applicable contract term without cost to the State. If the Services monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), the State shall be entitled to receive automatic credits as indicated immediately below, or the State may use other contractual remedies such as recovery of damages, as set forth herein in writing, e.g., in Specifications, Special Terms or in an SLA, and as such other contractual damages are limited by N.C.G.S. §143B-1350(h1) and the Limitation of Liability paragraph below. If not otherwise provided, the automatic remedies for nonavailability of the Subscription Services during a month are:
 - 1. A 10% service credit applied against future fees if Vendor does not reach 99.9% availability.
 - 2. A 25% service credit applied against future fees if Vendor does not reach 99% availability.
 - 3. A 50% service credit applied against future fees or eligibility for early termination of the Agreement if Vendor does not reach 95% availability.

If, however, Services meet the 99.9% service availability level for a month, but are not available for a consecutive 120 minutes during that month, the Vendor shall grant to the State a credit of a pro-rated one-day of the monthly subscription Services fee against future Services charges. Such credit(s) shall be applied to the bill immediately following the month in which Vendor failed to meet the performance requirements or other service levels; and the credit will continue to be deducted from the monthly invoice for each prior month that Vendor fails to meet the support response times for the remainder of the duration of the

Agreement. If Services monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, the State may also terminate the contract for material breach in accordance with the Default provisions hereinbelow.

- c) Support Services. If Vendor fails to meet Support Service response times as set forth herein or in an SLA for a period of three consecutive months, a 10% service credit will be deducted from the invoice in the month immediately following the third month, and the 10% service credit will continue to be deducted from the monthly invoice for each month that Vendor fails to meet the support response times for the remainder of the duration of the Agreement.

5) EXCLUSIONS:

- a) Except as stated above in Paragraphs 3 and 4, Vendor and its parent, subsidiaries and affiliates, subcontractors and suppliers make no warranties, express or implied, as to the Services.
- b) The warranties provided in Paragraphs 3 and 4 above do not cover repair for damages, malfunctions or service failures substantially caused by:
 - i) Actions of non-Vendor personnel;
 - ii) Failure to follow Vendor's written instructions relating to the Services provided to the State; or
 - iii) Force Majeure conditions set forth hereinbelow.
 - iv) The State's sole misuse of, or its own inability to use, the Services.

6) PERFORMANCE REVIEW AND ACCOUNTABILITY. N.C.G.S. § 143B-1340(f) and 09 NCAC 06B.1207 require provisions for performance review and accountability in State IT contracts. For this procurement, these shall include the holding a retainage of 10% of the contract value and withholding the final payment contingent on final acceptance by the State as provided in 09 NCAC 06B.1207(3) and (4), unless waived or otherwise agreed, in writing. The Services herein will be provided consistent with and under these Services performance review and accountability guarantees.

7) LIMITATION OF LIABILITY: Limitation of Vendor's Contract Damages Liability:

- a) Where Services are under the State's exclusive management and control, the Vendor shall not be liable for direct damages caused by the State's failure to fulfill any State responsibilities of assuring the proper use, management and supervision of the Services and programs, audit controls, operating methods, office procedures, or for establishing all proper checkpoints necessary for the State's intended use of the Services.
- b) The Vendor's liability for damages to the State arising under the contract shall be limited to two times the value of the Contract.
- c) The foregoing limitation of liability shall not apply to claims covered by other specific provisions including but not limited to Service Level Agreement or Deliverable/Product Warranty compliance, or to claims for injury to persons or damage to tangible personal property, gross negligence or willful or wanton conduct. This limitation of liability does not apply to contributions among joint tortfeasors under N.C.G.S. 1B-1 *et seq.*; the receipt of court costs or attorney's fees that might be awarded by a court in addition to damages after litigation based on this Contract. For avoidance of doubt, the Parties agree that the Service Level Agreement and Deliverable/Product Warranty Terms in the Contract are intended to provide the sole and exclusive remedies available to the State under the Contract for the Vendor's failure to comply with the requirements stated therein.

8) Vendor's Liability for Injury to Persons or Damage to Property:

- a) The Vendor shall be liable for damages arising out of personal injuries and/or damage to real or tangible personal property of the State, employees of the State, persons designated by the State for training, or person(s) other than agents or employees of the Vendor, designated by the State for any purpose, prior to, during, or subsequent to delivery, installation, acceptance, and use of the Services either at the Vendor's site or at the State's place of business, provided that the injury or damage was caused by the fault or negligence of the Vendor.

- b) The Vendor agrees to indemnify, defend and hold the Agency and the State and its Officers, employees, agents and assigns harmless from any liability relating to personal injury or injury to real or tangible personal property of any kind, accruing or resulting to any other person, firm or corporation furnishing or supplying work, Services, materials or supplies in connection with the performance of this Contract, whether tangible or intangible, arising out of the ordinary negligence, willful or wanton negligence, or intentional acts of the Vendor, its officers, employees, agents, assigns or subcontractors.
- c) Vendor shall not be liable for damages arising out of or caused by an alteration or an attachment not made or installed by the Vendor.

9) **MODIFICATION OF SERVICES:** If Vendor modifies or replaces the Services provided to the State and other tenants, and if the State has paid all applicable Subscription Fees, the State shall be entitled to receive, at no additional charge, access to a newer version of the Services that supports substantially the same functionality as the then accessible version of the Services. Newer versions of the Services containing substantially increased functionality may be made available to the State for an additional subscription fee. In the event of either of such modifications, the then accessible version of the Services shall remain fully available to the State until the newer version is provided to the State and accepted. If a modification materially affects the functionality of the Services as used by the State, the State, at its sole option, may defer such modification.

10) **TRANSITION PERIOD:**

- a) For ninety (90) days, either prior to the expiration date of this Agreement, or upon notice of termination of this Agreement, Vendor shall assist the State, upon written request, in extracting and/or transitioning all Data in the format determined by the State ("Transition Period").
- b) The Transition Period may be modified in an SLA or as agreed upon in writing by the parties in a contract amendment.
- c) During the Transition Period, Services access shall continue to be made available to the State without alteration.
- d) Vendor agrees to compensate the State for damages or losses the State incurs as a result of Vendor's failure to comply with this Transition Period section in accordance with the Limitation of Liability provisions above.
- e) Upon termination, and unless otherwise stated in an SLA, and after providing the State Data to the State as indicated above in this section with acknowledged receipt by the State in writing, the Vendor shall permanently destroy or render inaccessible any portion of the State Data in Vendor's and/or subcontractor's possession or control following the completion and expiration of all obligations in this section. Within thirty (30) days, Vendor shall issue a written statement to the State confirming the destruction or inaccessibility of the State's Data.
- f) The State at its option, may purchase additional Transition services as may be agreed upon in a supplemental agreement.

11) **TRANSPORTATION:** Transportation charges for any Deliverable sent to the State other than electronically or by download, shall be FOB Destination unless delivered by internet or file-transfer as agreed by the State, or otherwise specified in the solicitation document or purchase order.

12) **TRAVEL EXPENSES:** All travel expenses should be included in the Vendor's proposed costs. Separately stated travel expenses will not be reimbursed. In the event that the Vendor may be eligible to be reimbursed for travel expenses specifically agreed to in writing and arising under the performance of this Agreement, reimbursement will be at the out-of-state rates set forth in G.S. §138-6; as amended from time to time. Vendor agrees to use the lowest available airfare not requiring a weekend stay and to use the lowest available rate for rental vehicles. All Vendor incurred travel expenses shall be billed on a monthly basis, shall be supported by receipt and shall be paid by the State within thirty (30) days after invoice approval. Travel expenses exceeding the foregoing rates shall not be paid by the State. The State will reimburse travel allowances only for days on which the Vendor is required to be in North Carolina performing Services under this Agreement.

13) **PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES:** Vendor warrants that it has not paid, and agrees not to pay, any bonus, commission, fee, or gratuity to any employee or

official of the State for the purpose of obtaining any contract or award issued by the State. Subsequent discovery by the State of non-compliance with these provisions shall constitute sufficient cause for immediate termination of all outstanding Agreements with the Vendor. Violations of this provision may result in debarment of the Vendor(s) or Vendor(s) as permitted by 9 NCAC 06B.1207, or other provision of law.

14) **AVAILABILITY OF FUNDS:** Any and all payments by the State are expressly contingent upon and subject to the appropriation, allocation and availability of funds to the State for the purposes set forth in this Agreement. If this Agreement or any Purchase Order issued hereunder is funded in whole or in part by federal funds, the State's performance and payment shall be subject to and contingent upon the continuing availability of said federal funds for the purposes of the Agreement or Purchase Order. If the term of this Agreement extends into fiscal years subsequent to that in which it is approved such continuation of the Agreement *is expressly contingent upon* the appropriation, allocation, and availability of funds by the N.C. Legislature for the purposes set forth in the Agreement. If funds to effect payment are not available, the State will provide written notification to Vendor. If the Agreement is terminated under this paragraph, Vendor agrees to terminate any Services supplied to the State under this Agreement, and relieve the State of any further obligation thereof. The State shall remit payment for Services accepted on or prior to the date of the aforesaid notice in conformance with the payment terms.

15) **PAYMENT TERMS:**

- a) Payment may be made by the State in advance of or in anticipation of subscription Services to be actually performed under the Agreement or upon proper invoice for other Services rendered. Payment terms are Net 30 days after receipt of correct invoice. Initial payments are to be made after final acceptance of the Services. Payments are subject to any retainage requirements herein. The Purchasing State Agency is responsible for all payments under the Agreement. Subscription fees for term years after the initial year shall be as quoted under State options herein, but shall not increase more than 5% over the prior term, except as the parties may have agreed to an alternate formula to determine such increases in writing. No additional charges to the State will be permitted based upon, or arising from, the State's use of a Business Procurement Card. The State may exercise any and all rights of Set Off as permitted in Chapter 105A-1 *et seq.* of the N.C. General Statutes and applicable Administrative Rules.
- b) Upon Vendor's written request of not less than 30 days and approval by the State, the State may:
 - i) Forward the Vendor's payment check(s) directly to any person or entity designated by the Vendor, or
 - ii) Include any person or entity designated in writing by Vendor as a joint payee on the Vendor's payment check(s), however,
 - iii) In no event shall such approval and action obligate the State to anyone other than the Vendor and the Vendor shall remain responsible for fulfillment of all Agreement obligations.
- c) For any third party software licensed by Vendor or its subcontractors for use by the State, a copy of the software license including terms acceptable to the State, an assignment acceptable to the State, and documentation of license fees paid by the Vendor must be provided to the State before any related license fees or costs may be billed to the State.
- d) An undisputed invoice is an invoice for which the State and/or the Purchasing State Agency has not disputed in writing within thirty (30) days from the invoice date, unless the agency requests more time for review of the invoice. Upon Vendor's receipt of a disputed invoice notice, Vendor will work to correct the applicable invoice error, provided that such dispute notice shall not relieve the State or the applicable Purchasing State Agency from its payment obligations for the undisputed items on the invoice or for any disputed items that are ultimately corrected. The Purchasing State Agency is not required to pay the Vendor for any Software or Services provided without a written purchase order from the appropriate Purchasing State Agency. In addition, all such Services provided must meet all terms, conditions, and specifications of this Agreement and purchase order and be accepted as satisfactory by the Purchasing State Agency before payment will be issued.

- e) The Purchasing State Agency shall release any amounts held as retainages for Services completed within a reasonable period after the end of the period(s) or term(s) for which the retainage was withheld. Payment retainage shall apply to all invoiced items, excepting only such items as Vendor obtains from Third Parties and for which costs are chargeable to the State by agreement of the Parties. The Purchasing State Agency, in its sole discretion, may release retainages withheld from any invoice upon acceptance of the Services identified or associated with such invoices.

16) ACCEPTANCE CRITERIA:

- a) Initial acceptance testing is required for all Vendor supplied Services before going live, unless provided otherwise in the solicitation documents or a Statement of Work. The State may define such processes and procedures as may be necessary or proper, in its opinion and discretion, to ensure compliance with the State's specifications and Vendor's technical representations. Acceptance of Services may be controlled by additional written terms as agreed by the parties.
- b) After initial acceptance of Services, the State shall have the obligation to notify Vendor, in writing and within ten (10) days following provision of any Deliverable described in the contract if it is not acceptable. The notice shall specify in reasonable detail the reason(s) a Deliverable is unacceptable. Acceptance by the State of any Vendor re-performance or correction shall not be unreasonably withheld, but may be conditioned or delayed as required for confirmation by the State that the issue(s) in the notice have been successfully corrected.

17) CONFIDENTIALITY: The State may maintain the confidentiality of certain types of information described in N.C. Gen. Stat. §132-1, *et seq.* Such information may include trade secrets defined by N.C. Gen. Stat. §66-152 and other information exempted from the Public Records Act pursuant to N.C. Gen. Stat. §132-1.2. Vendor may designate information, Products, Services or appropriate portions of its response as confidential, consistent with and to the extent permitted under the Statutes and Rules set forth above, by marking the top and bottom of pages containing confidential information with a legend in boldface type "**CONFIDENTIAL.**" By so marking any page, or portion of a page, the Vendor warrants that it has formed a good faith opinion, having received such necessary or proper review by counsel and other knowledgeable advisors, that the portions marked "confidential" meet the requirements of the Rules and Statutes set forth above. **However, under no circumstances shall price information be designated as confidential.** The State agrees to promptly notify the Vendor in writing of any action seeking to compel the disclosure of Vendor's confidential information. If an action is brought pursuant to N.C. Gen. Stat. §132-9 to compel the State to disclose information marked "confidential," the Vendor agrees that it will intervene in the action through its counsel and participate in defending the State, including any public official(s) or public employee(s). The Vendor agrees that it shall hold the State and any official(s) and individual(s) harmless from any and all damages, costs, and attorneys' fees awarded against the State in the action. The State shall have the right, at its option and expense, to participate in the defense of the action through its counsel. The State shall have no liability to Vendor with respect to the disclosure of Vendor's confidential information ordered by a court of competent jurisdiction pursuant to N.C. Gen. Stat. §132-9 or other applicable law.

18) SECURITY OF STATE DATA:

- a) All materials, including software, Data, information and documentation provided by the State to the Vendor (State Data) during the performance or provision of Services hereunder are the property of the State of North Carolina and must be kept secure and returned to the State. The Vendor will protect State Data in its hands from unauthorized disclosure, loss, damage, destruction by natural event, or other eventuality. Proprietary Vendor materials shall be identified to the State by Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be provided to the State as part of the Services. The Vendor shall not access State User accounts, or State Data, except (i) during data center operations, (ii) in response to service or technical issues, (iii) as required by the express terms of this contract, or (iv) at State's written request. The Vendor shall protect the confidentiality of all information, Data, instruments, studies, reports, records and other materials provided to it

by the State or maintained or created in accordance with this Agreement. No such information, Data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written agreement with the State. The Vendor will have written policies governing access to and duplication and dissemination of all such information, Data, instruments, studies, reports, records and other materials.

- b) The Vendor shall not store or transfer non-public State data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State of North Carolina data remotely only as required to provide technical support.
- c) Protection of personal privacy and sensitive data. The Vendor acknowledges its responsibility for securing any restricted or highly restricted data, as defined by the Statewide Data Classification and Handling Policy (<https://it.nc.gov/document/statewide-data-classification-and-handling-policy>) that is collected by the State and stored in any Vendor site or other Vendor housing systems including, but not limited to, computer systems, networks, servers, or databases, maintained by Vendor or its agents or subcontractors in connection with the provision of the Services. The Vendor warrants, at its sole cost and expense, that it shall implement processes and maintain the security of data classified as restricted or highly restricted; provide reasonable care and efforts to detect fraudulent activity involving the data; and promptly notify the State of any breaches of security within 24 hours of confirmation as required by N.C.G.S. § 143B-1379.
- d) The Vendor will provide and maintain secure backup of the State Data. The Vendor shall implement and maintain secure passwords for its online system providing the Services, as well as all appropriate administrative, physical, technical and procedural safeguards at all times during the term of this Agreement to secure such Data from Data Breach, protect the Data and the Services from loss, corruption, unauthorized disclosure, and the introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data and the Services. The Vendor will allow periodic back-up of State Data by the State to the State's infrastructure as the State requires or as may be provided by law.
- e) The Vendor shall certify to the State:
 - i. The sufficiency of its security standards, tools, technologies and procedures in providing Services under this Agreement;
 - ii. That the system used to provide the Subscription Services under this Contract has and will maintain a valid 3rd party security certification not to exceed 1 year and is consistent with the data classification level and a security controls appropriate for low or moderate information system(s) per the National Institute of Standards and Technology NIST 800-53 revision 4. The State reserves the right to independently evaluate, audit, and verify such requirements.
 - iii. That the Services will comply with the following:
 - (1) Any DIT security policy regarding Cloud Computing, and the DIT Statewide Information Security Policy Manual; to include encryption requirements as defined below:
 - (a) The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.
 - (b) For engagements where the Vendor stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. Examples are social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. The Vendor's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the Service Provider cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security

liability insurance coverage for any loss resulting from a data breach. Additionally, where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection;

- (2) Privacy provisions of the Federal Privacy Act of 1974;
 - (3) The North Carolina Identity Theft Protection Act, N.C.G.S. Chapter 75, Article 2A (e.g., N.C.G.S. § 75-65 and -66);
 - (4) The North Carolina Public Records Act, N.C.G.S. Chapter 132; and
 - (5) Applicable Federal, State and industry standards and guidelines including, but not limited to, relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines, Criminal Justice Information, The Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA);
 - (6) Any requirements implemented by the State under N.C.G.S. §§ 143B-1376 and -1377.
- f) **Security Breach.** "Security Breach" under the NC Identity Theft Protection Act (N.C.G.S. § 75-60ff) means (1) any circumstance pursuant to which applicable Law requires notification of such breach to be given to affected parties or other activity in response to such circumstance (e.g., N.C.G.S. § 75-65); or (2) any actual, attempted, suspected, threatened, or reasonably foreseeable circumstance that compromises, or could reasonably be expected to compromise, either Physical Security or Systems Security (as such terms are defined below) in a fashion that either does or could reasonably be expected to permit unauthorized Processing (as defined below), use, disclosure or acquisition of or access to any the State Data or state confidential information. "Physical Security" means physical security at any site or other location housing systems maintained by Vendor or its agents or subcontractors in connection with the Services. "Systems Security" means security of computer, electronic or telecommunications systems of any variety (including data bases, hardware, software, storage, switching and interconnection devices and mechanisms), and networks of which such systems are a part or communicate with, used directly or indirectly by Vendor or its agents or subcontractors in connection with the Services. "Processing" means any operation or set of operations performed upon the State Data or State confidential information, whether by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing or destroying.
- g) **Breach Notification.** In the event Vendor becomes aware of any Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall, at its own expense, (1) immediately notify the State's Agreement Administrator of such Security Breach and perform a root cause analysis thereon, (2) investigate such Security Breach, (3) provide a remediation plan, acceptable to the State, to address the Security Breach and prevent any further incidents, (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (5) cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach. The State shall make the final decision on notifying the State's persons, entities, employees, service providers and/or the public of such Security Breach, and the implementation of the remediation plan. If a notification to a customer is required under any Law or pursuant to any of the State's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by the State) shall be considered legally required.
- h) **Notification Related Costs.** Vendor shall reimburse the State for all Notification Related Costs incurred by the State arising out of or in connection with any such Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement resulting in a requirement for legally required notifications. "Notification Related Costs" shall include the State's internal and external costs associated with addressing and responding to the Security Breach, including but not limited to: (1) preparation and mailing

or other transmission of legally required notifications; (2) preparation and mailing or other transmission of such other communications to customers, agents or others as the State deems reasonably appropriate; (3) establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training); (4) public relations and other similar crisis management services; (5) legal and accounting fees and expenses associated with the State's investigation of and response to such event; and (6) costs for credit reporting services that are associated with legally required notifications or are advisable, in the State's opinion, under the circumstances. In the event that Vendor becomes aware of any Security Breach which is not due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall immediately notify the State of such Security Breach, and the parties shall reasonably cooperate regarding which of the foregoing or other activities may be appropriate under the circumstances, including any applicable Charges for the same.

- i) Vendor shall allow the State reasonable access to Services security logs, latency statistics, and other related Services security data that affect this Agreement and the State's Data, at no cost to the State.
- j) In the course of normal operations, it may become necessary for Vendor to copy or move Data to another storage destination on its online system, and delete the Data found in the original location. In any such event, the Vendor shall preserve and maintain the content and integrity of the Data, except by prior written notice to, and prior written approval by, the State.
- k) Remote access to Data from outside the continental United States, including, without limitation, remote access to Data by authorized Services support staff in identified support centers, is prohibited unless approved in advance by the State Chief Information Officer or the Using Agency.
- l) In the event of temporary loss of access to Services, Vendor shall promptly restore continuity of Services, restore Data in accordance with this Agreement and as may be set forth in an SLA, restore accessibility of Data and the Services to meet the performance requirements stated herein or in an SLA. As a result, Service Level remedies will become available to the State as provided herein, in the SLA or other agreed and relevant documents. Failure to promptly remedy any such temporary loss of access may result in the State exercising its options for assessing damages under this Agreement.
- m) In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to Data or Services, Vendor shall notify the State by the fastest means available and also in writing, with additional notification provided to the State Chief Information Officer or designee of the contracting agency. Vendor shall provide such notification within twenty-four (24) hours after Vendor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Vendor shall inform the State of:
 - 1) The scale and quantity of the State Data loss;
 - 2) What Vendor has done or will do to recover the State Data from backups and mitigate any deleterious effect of the State Data and Services loss; and
 - 3) What corrective action Vendor has taken or will take to prevent future State Data and Services loss.
 - 4) If Vendor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Agreement.Vendor shall conduct an investigation of the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Vendor shall cooperate fully with the State, its agents and law enforcement.
- n) In the event of termination of this contract, cessation of business by the Vendor or other event preventing Vendor from continuing to provide the Services, Vendor shall not withhold the State Data or any other State confidential information or refuse for any reason, to promptly return to the State the State Data and any other State confidential information (including copies thereof) if requested to do so on such media as reasonably requested by the State, even if the State is then or is alleged to be in breach of the Agreement. As a part of Vendor's obligation to provide the State Data pursuant to this Paragraph 18) n),

Vendor will also provide the State any data maps, documentation, software, or other materials necessary, including, without limitation, handwritten notes, materials, working papers or documentation, for the State to use, translate, interpret, extract and convert the State Data.

- o) **Secure Data Disposal.** When requested by the State, the Vendor shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods and certificates of destruction shall be provided to the State.

19) **ACCESS TO PERSONS AND RECORDS:** Pursuant to N.C. General Statute 147-64.7, the State, the State Auditor, appropriate federal officials, and their respective authorized employees or agents are authorized to examine all books, records, and accounts of the Vendor insofar as they relate to transactions with any department, board, officer, commission, institution, or other agency of the State of North Carolina pursuant to the performance of this Agreement or to costs charged to this Agreement. The Vendor shall retain any such books, records, and accounts for a minimum of three (3) years after the completion of this Agreement. Additional audit or reporting requirements may be required by any State, if in the State's opinion, such requirement is imposed by federal or state law or regulation. The Vendor shall allow the State to audit conformance including contract terms, system security and data centers as appropriate. The State may perform this audit or contract with a third party at its discretion at the State's expense. Such reviews shall be conducted with at least 30 days' advance written notice and shall not unreasonably interfere with the Service Provider's business.

20) **ASSIGNMENT:** Vendor may not assign this Agreement or its obligations hereunder except as permitted by 09 NCAC 06B.1003 and this Paragraph. Vendor shall provide reasonable notice of not less than thirty (30) days of any consolidation, acquisition, or merger. Any assignee shall affirm this Agreement attorning to the terms and conditions agreed, and that Vendor shall affirm that the assignee is fully capable of performing all obligations of Vendor under this Agreement. An assignment may be made, if at all, in writing by the Vendor, Assignee and the State setting forth the foregoing obligation of Vendor and Assignee.

21) **NOTICES:** Any notices required under this Agreement should be delivered to the Agreement Administrator for each party. Unless otherwise specified in the Solicitation Documents, any notices shall be delivered in writing by U.S. Mail, Commercial Courier, facsimile or by hand.

22) **TITLES AND HEADINGS:** Titles and Headings in this Agreement are used for convenience only and do not define, limit or proscribe the language of terms identified by such Titles and Headings.

23) **AMENDMENT:** This Agreement may not be amended orally or by performance. Any amendment must be made in written form and signed by duly authorized representatives of the State and Vendor.

24) **TAXES:** The State of North Carolina is exempt from Federal excise taxes and no payment will be made for any personal property taxes levied on the Vendor or for any taxes levied on employee wages. Agencies of the State may have additional exemptions or exclusions for federal or state taxes. Evidence of such additional exemptions or exclusions may be provided to Vendor by Agencies, as applicable, during the term of this Agreement. Applicable State or local sales taxes shall be invoiced as a separate item.

25) **GOVERNING LAWS, JURISDICTION, AND VENUE:** This Agreement is made under and shall be governed and construed in accordance with the laws of the State of North Carolina. The place of this Agreement or purchase order, its situs and forum, shall be Wake County, North Carolina, where all matters, whether sounding in contract or in tort, relating to its validity, construction, interpretation and enforcement shall be determined. Vendor agrees and submits, solely for matters relating to this Agreement, to the jurisdiction of the courts of the State of North Carolina, and stipulates that Wake County shall be the proper venue for all matters.

26) **DEFAULT:** In the event Services or other Deliverable furnished or performed by the Vendor during performance of any Contract term fail to conform to any material requirement(s) of the Contract specifications, notice of the failure is provided by the State and if the failure is not cured within ten (10) days, or Vendor fails to meet the material requirements and specifications herein, the State may cancel the contract. Default may be cause for debarment as provided in 09 NCAC

06B.1206. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.

- a) If Vendor fails to deliver or provide correct Services within the time required by this Contract, the State shall provide written notice of said failure to Vendor, and by such notice require performance assurance measures pursuant to N.C.G.S. 143B-1340(f). Vendor is responsible for the delays resulting from its failure to deliver or provide Services as provided herein.
- b) Should the State fail to perform any of its obligations upon which Vendor's performance is conditioned, Vendor shall not be in default for any delay, cost increase or other consequences resulting from the State's failure. Vendor will use reasonable efforts to mitigate delays, costs or expenses arising from assumptions in the Vendor's offer documents that prove erroneous or are otherwise invalid. Any deadline that is affected by any such Vendor failure in assumptions or performance by the State shall be extended by an amount of time reasonably necessary to compensate for the effect of such failure. Vendor shall provide a plan to cure any delay or default if requested by the State. The plan shall state the nature of the delay or default, the time required for cure, any mitigating factors causing or tending to cause the delay or default, and such other information as the Vendor may deem necessary or proper to provide.

27) **FORCE MAJEURE:** Except as provided for herein, neither party shall be deemed to be in default of its obligations hereunder if and so long as it is prevented from performing such obligations as a result of events beyond its reasonable control, including without limitation, fire, power failures, any act of war, hostile foreign action, nuclear explosion, riot, strikes or failures or refusals to perform under subcontracts, civil insurrection, earthquake, hurricane, tornado, or other catastrophic natural event or act of God.

28) **COMPLIANCE WITH LAWS:** The Vendor shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business and the provision of Services hereunder, including those of federal, state, and local agencies having jurisdiction and/or authority.

29) **TERMINATION:** Any notice or termination made under this Agreement shall be transmitted via US Mail, Certified Return Receipt Requested. The period of notice for termination shall begin on the day the return receipt is signed and dated. The parties may mutually terminate this Agreement by written agreement at any time.

- a) The State may terminate this Agreement, in whole or in part, pursuant to the Paragraph entitled "Default," above, or pursuant to Special Terms and Conditions in the Solicitation Documents, if any, or for any of the following
 - i) **Termination for Cause:** In the event any goods, Services, or service furnished by the Vendor during performance fails to conform to any material specification or requirement of the Agreement, and the failure is not cured within the specified time after providing written notice thereof to Vendor, the State may cancel and procure the articles or Services from other sources; holding Vendor liable for any excess costs occasioned thereby, subject only to the limitations provided in Paragraph 7), entitled "Limitation of Liability." The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Agreement. Vendor shall not be relieved of liability to the State for damages sustained by the State arising from Vendor's breach of this Agreement; and the State may, in its discretion, withhold any payment due as a setoff until such time as the damages are finally determined or as agreed by the parties. Voluntary or involuntary Bankruptcy or receivership by Vendor shall be cause for termination.
 - ii) **Termination for Convenience Without Cause:** The State may terminate service and indefinite quantity contracts; in whole or in part by giving thirty (30) days prior notice in writing to the Vendor. Vendor shall be entitled to sums due as compensation for Services performed in conformance with the Agreement. In the event the Agreement is terminated for the convenience of the State the State will pay for all Services and work performed or delivered in conformance with the Agreement up to the date of termination.

30) **DISPUTE RESOLUTION:** The parties agree that it is in their mutual interest to resolve disputes informally. A claim by the State shall be submitted in writing to the Vendor's Agreement Administrator for decision. The Parties shall negotiate in good faith and use all reasonable efforts to resolve such dispute(s). During the time the Parties are attempting to resolve any dispute, each shall proceed diligently to perform their respective duties and responsibilities under this Agreement. If a dispute cannot be resolved between the Parties within thirty (30) days after delivery of notice, either Party may elect to exercise any other remedies available under this Agreement, or at law. This term shall not constitute an agreement by either party to mediate or arbitrate any dispute.

31) **SEVERABILITY:** In the event that a court of competent jurisdiction holds that a provision or requirement of this Agreement violates any applicable law, each such provision or requirement shall be enforced only to the extent it is not in violation of law or is not otherwise unenforceable and all other provisions and requirements of this Agreement shall remain in full force and effect. All promises, requirement, terms, conditions, provisions, representations, guarantees and warranties contained herein shall survive the expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable federal or State statute, including statutes of repose or limitation.

32) **FEDERAL INTELLECTUAL PROPERTY BANKRUPTCY PROTECTION ACT:** The Parties agree that the State shall be entitled to any and all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto.

33) **ELECTRONIC PROCUREMENT:** (Applies to all contracts that include E-Procurement and are identified as such in the body of the solicitation document): Purchasing shall be conducted through the Statewide E-Procurement Service. The State's third-party agent shall serve as the Supplier Manager for this E-Procurement Service. The Vendor shall register for the Statewide E-Procurement Service within two (2) business days of notification of award in order to receive an electronic purchase order resulting from award of this contract. The E-Procurement fee does not normally apply to services.

- a) Reserved.
- b) Reserved.
- c) The Supplier Manager will capture the order from the State approved user, including the shipping and payment information, and submit the order in accordance with the E-Procurement Service. Subsequently, the Supplier Manager will send those orders to the appropriate Vendor on State Agreement. The State or State approved user, not the Supplier Manager, shall be responsible for the solicitation, bids received, evaluation of bids received, award of contract, and the payment for goods delivered.
- d) Vendor agrees at all times to maintain the confidentiality of its user name and password for the Statewide E-Procurement Services. If a Vendor is a corporation, partnership or other legal entity, then the Vendor may authorize its employees to use its password. Vendor shall be responsible for all activity and all charges for such employees. Vendor agrees not to permit a third party to use the Statewide E-Procurement Services through its account. If there is a breach of security through the Vendor's account, Vendor shall immediately change its password and notify the Supplier Manager of the security breach by e-mail. Vendor shall cooperate with the state and the Supplier Manager to mitigate and correct any security breach.

The following terms and conditions apply to Software as a Service (SaaS) solutions.

1) DEFINITIONS:

- a) "Data" includes means information, formulae, algorithms, or other content that the State, the State's employees, agents and end users upload, create or modify using the Services pursuant to this Agreement. Data also includes user identification information and metadata which may contain Data or from which the State's Data may be ascertainable.

- b) Deliverable/Product Warranties shall mean and include the warranties provided for products or deliverables licensed to the State as included in Paragraph 7) c) of these Terms and Conditions unless superseded by a Vendor's Warranties pursuant to Vendor's License or Support Agreements.
- c) "Services" shall mean the duties and tasks undertaken by the Vendor to fulfill the requirements and specifications of this solicitation, including, without limitation, providing web browser access by authorized users to certain Vendor online software applications identified herein, and to related services, such as Vendor hosted Computer storage, databases, Support, documentation, and other functionalities, all as a Software as a Service ("SaaS") solution.
- d) "State" shall mean the State of North Carolina, the Department of Information Technology as an agency, or the agency identified in this solicitation as the Purchasing Agency and Award Authority.
- e) "Support" includes provision of ongoing updates and maintenance for the Vendor online software applications, and as may be specified herein, consulting, training and other support Services as provided by the Vendor for SaaS tenants receiving similar SaaS Services.

2) ACCESS AND USE OF SAAS SERVICES:

- a) Vendor grants the State a personal non-transferable and non-exclusive right to use and access, all Services and other functionalities or services provided, furnished or accessible under this Agreement. The State may utilize the Services as agreed herein and in accordance with any mutually agreed Acceptable Use Policy. The State is authorized to access State Data and any Vendor-provided data as specified herein and to transmit revisions, updates, deletions, enhancements, or modifications to the State Data. This shall include the right of the State to, and access to, Support without the Vendor requiring a separate maintenance or support agreement. Subject to an agreed limitation on the number of users, the State may use the Services with any computer, computer system, server, or desktop workstation owned or utilized by the State or other authorized users. User access to the Services shall be routinely provided by the Vendor and may be subject to a more specific Service Level Agreement (SLA) agreed to in writing by the parties. The State shall notify the Vendor of any unauthorized use of any password or account, or any other known or suspected breach of security access. The State also agrees to refrain from taking any steps, such as reverse engineering, reverse assembly or reverse compilation to derive a source code equivalent to the Services or any portion thereof. Use of the Services to perform services for commercial third parties (so-called "service bureau" uses) is not permitted, but the State may utilize the Services to perform its governmental functions. If the Services fees are based upon the number of Users and/or hosted instances, the number of Users/hosted instances available may be adjusted at any time (subject to the restrictions on the maximum number of Users specified in the Furnish and Deliver Table herein above) by mutual agreement and State Procurement approval. All Services and information designated as "confidential" or "proprietary" shall be kept in confidence except as may be required by the North Carolina Public Records Act: N.C.G.S. § 132-1, *et. seq.*
- b) The State's access license for the Services and its associated services neither transfers, vests, nor infers any title or other ownership right in any intellectual property rights of the Vendor or any third party, nor does this license transfer, vest, or infer any title or other ownership right in any source code associated with the Services unless otherwise agreed to by the parties. The provisions of this paragraph will not be construed as a sale of any ownership rights in the Services. Any Services or technical and business information owned by Vendor or its suppliers or licensors made accessible or furnished to the State shall be and remain the property of the Vendor or such other party, respectively. Vendor has a limited, non-exclusive license to access and use the State Data as provided to Vendor, but solely for performing its obligations under this Agreement and in confidence as provided herein.
- c) Vendor or its suppliers shall at minimum, and except as otherwise agreed, provide telephone assistance to the State for all Services procured hereunder during the State's normal business hours (unless different hours are specified herein). Vendor warrants that

its Support and customer service and assistance will be performed in accordance with generally accepted industry standards. The State has the right to receive the benefit of upgrades, updates, maintenance releases or other enhancements or modifications made generally available to Vendor's SaaS tenants for similar Services. Vendor's right to a new use agreement for new version releases of the Services shall not be abridged by the foregoing. Vendor may, at no additional charge, modify the Services to improve operation and reliability or to meet legal requirements.

- d) Vendor will provide to the State the same Services for updating, maintaining and continuing optimal performance for the Services as provided to other similarly situated users or tenants of the Services, but minimally as provided for and specified herein. Unless otherwise agreed in writing, Support will also be provided for any other (e.g., third-party) software provided by the Vendor in connection with the Vendor's solution herein. The technical and professional activities required for establishing, managing, and maintaining the Services environment are the responsibilities of the Vendor. Any training specified herein will be provided by the Vendor to certain State users for the fees or costs as set forth herein or in an SLA.
 - e) Services provided pursuant to this Solicitation may, in some circumstances, be accompanied by a user clickwrap agreement. The term clickwrap agreement refers to an agreement that requires the end user to manifest his or her assent to terms and conditions by clicking an "ok" or "agree" button on a dialog box or pop-up window as part of the process of access to the Services. All terms and conditions of any clickwrap agreement provided with any Services solicited herein shall have no force and effect and shall be non-binding on the State, its employees, agents, and other authorized users of the Services.
 - f) The Vendor may utilize partners and/or subcontractors to assist in the provision of the Services, so long as the State Data is not removed from the United States unless the terms of storage of the State Data are clearly disclosed, the security provisions referenced herein can still be complied with, and such removal is done with the prior express written permission of the State. The Vendor shall identify all of its strategic business partners related to Services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.
 - g) Vendor warrants that all Services will be performed with professional care and skill, in a workmanlike manner and in accordance with the Services documentation and this Agreement.
 - h) An SLA or other agreed writing shall contain provisions for scalability of Services and any variation in fees or costs as a result of any such scaling.
 - i) Professional services provided by the Vendor at the request by the State in writing in addition to agreed Services shall be at the then-existing Vendor hourly rates when provided, unless otherwise agreed in writing by the parties.
- 3) **WARRANTY OF NON-INFRINGEMENT; REMEDIES.**
- a) Vendor warrants to the best of its knowledge that:
 - i) The Services do not infringe any intellectual property rights of any third party; and
 - ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party;
 - b) Should any Services supplied by Vendor become the subject of a claim of infringement of a patent, copyright, Trademark or a trade secret in the United States, the Vendor, shall at its option and expense, either procure for the State the right to continue using the Services, or replace or modify the same to become noninfringing. If neither of these options can reasonably be taken in Vendor's judgment, or if further use shall be prevented by injunction, the Vendor agrees to cease provision of any affected Services, and refund any sums the State has paid Vendor and make every reasonable effort to assist the State in procuring substitute Services. If, in the sole opinion of the State, the cessation of use by the State of any such Services due to infringement issues makes the retention of other items acquired from the Vendor under this Agreement impractical, the State shall then have the option of

terminating the Agreement, or applicable portions thereof, without penalty or termination charge; and Vendor agrees to refund any sums the State paid for unused Services.

- c) The Vendor, at its own expense, shall defend any action brought against the State to the extent that such action is based upon a claim that the Services supplied by the Vendor, their use or operation, infringes on a patent, copyright, trademark or violates a trade secret in the United States. The Vendor shall pay those costs and damages finally awarded or agreed in a settlement against the State in any such action. Such defense and payment shall be conditioned on the following:
 - i) That the Vendor shall be notified within a reasonable time in writing by the State of any such claim; and,
 - ii) That the Vendor shall have the sole control of the defense of any action on such claim and all negotiations for its settlement or compromise provided, however, that the State shall have the option to participate in such action at its own expense.
- d) Vendor will not be required to defend or indemnify the State if any claim by a third party against the State for infringement or misappropriation results from the State's material alteration of any Vendor-branded Services, or from the continued use of the good(s) or Services after receiving notice they infringe on a trade secret of a third party.

4) ACCESS AVAILABILITY; REMEDIES:

- a) The Vendor warrants that the Services will be in good working order, and operating in conformance with Vendor's standard specifications and functions as well as any other specifications agreed to by the parties in writing, and shall remain accessible 24/7, with the exception of scheduled outages for maintenance and of other service level provisions agreed in writing, e.g., in an SLA. Vendor does not warrant that the operation of the Services will be completely uninterrupted or error free, or that the Services functions will meet all the State's requirements, unless developed as Customized Services.
- b) The State shall notify the Vendor if the Services are not in good working order or inaccessible during the term of the Agreement. Vendor shall, at its option, either repair, replace or reperform any Services reported or discovered as not being in good working order and accessible during the applicable contract term without cost to the State. If the Services monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), the State shall be entitled to receive automatic credits as indicated immediately below, or the State may use other contractual remedies such as recovery of damages, as set forth herein in writing, e.g., in Specifications, Special Terms or in an SLA, and as such other contractual damages are limited by N.C.G.S. §143B-1350(h1) and the Limitation of Liability paragraph below. If not otherwise provided, the automatic remedies for nonavailability of the Subscription Services during a month are:
 - 1. A 10% service credit applied against future fees if Vendor does not reach 99.9% availability.
 - 2. A 25% service credit applied against future fees if Vendor does not reach 99% availability.
 - 3. A 50% service credit applied against future fees or eligibility for early termination of the Agreement if Vendor does not reach 95% availability.

If, however, Services meet the 99.9% service availability level for a month, but are not available for a consecutive 120 minutes during that month, the Vendor shall grant to the State a credit of a pro-rated one-day of the monthly subscription Services fee against future Services charges. Such credit(s) shall be applied to the bill immediately following the month in which Vendor failed to meet the performance requirements or other service levels, and the credit will continue to be deducted from the monthly invoice for each prior month that Vendor fails to meet the support response times for the remainder of the duration of the Agreement. If Services monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, the State may also terminate the contract for material breach in accordance with the Default provisions hereinbelow.

- c) Support Services. If Vendor fails to meet Support Service response times as set forth herein or in an SLA for a period of three consecutive months, a 10% service credit will be deducted from the invoice in the month immediately following the third month, and the 10%

service credit will continue to be deducted from the monthly invoice for each month that Vendor fails to meet the support response times for the remainder of the duration of the Agreement.

5) EXCLUSIONS:

- c) Except as stated above in Paragraphs 3 and 4, Vendor and its parent, subsidiaries and affiliates, subcontractors and suppliers make no warranties, express or implied, as to the Services.
- d) The warranties provided in Paragraphs 3 and 4 above do not cover repair for damages, malfunctions or service failures substantially caused by:
 - i) Actions of non-Vendor personnel;
 - ii) Failure to follow Vendor's written instructions relating to the Services provided to the State; or
 - iii) Force Majeure conditions set forth hereinbelow.
 - iv) The State's sole misuse of, or its own inability to use, the Services.

6) PERFORMANCE REVIEW AND ACCOUNTABILITY. N.C.G.S. § 143B-1340(f) and 09 NCAC 06B.1207 require provisions for performance review and accountability in State IT contracts. For this procurement, these shall include the holding a retainage of 10% of the contract value and withholding the final payment contingent on final acceptance by the State as provided in 09 NCAC 06B.1207(3) and (4), unless waived or otherwise agreed, in writing. The Services herein will be provided consistent with and under these Services performance review and accountability guarantees.

7) LIMITATION OF LIABILITY: Limitation of Vendor's Contract Damages Liability:

- a) Where Services are under the State's exclusive management and control, the Vendor shall not be liable for direct damages caused by the State's failure to fulfill any State responsibilities of assuring the proper use, management and supervision of the Services and programs, audit controls, operating methods, office procedures, or for establishing all proper checkpoints necessary for the State's intended use of the Services.
- b) The Vendor's liability for damages to the State arising under the contract shall be limited to two times the value of the Contract.
- c) The foregoing limitation of liability shall not apply to claims covered by other specific provisions including but not limited to Service Level Agreement or Deliverable/Product Warranty compliance, or to claims for injury to persons or damage to tangible personal property, gross negligence or willful or wanton conduct. This limitation of liability does not apply to contributions among joint tortfeasors under N.C.G.S. 1B-1 et seq., the receipt of court costs or attorney's fees that might be awarded by a court in addition to damages after litigation based on this Contract. For avoidance of doubt, the Parties agree that the Service Level Agreement and Deliverable/Product Warranty Terms in the Contract are intended to provide the sole and exclusive remedies available to the State under the Contract for the Vendor's failure to comply with the requirements stated therein.

8) Vendor's Liability for Injury to Persons or Damage to Property:

- a) The Vendor shall be liable for damages arising out of personal injuries and/or damage to real or tangible personal property of the State, employees of the State, persons designated by the State for training, or person(s) other than agents or employees of the Vendor, designated by the State for any purpose, prior to, during, or subsequent to delivery, installation, acceptance, and use of the Services either at the Vendor's site or at the State's place of business, provided that the injury or damage was caused by the fault or negligence of the Vendor.
- b) The Vendor agrees to indemnify, defend and hold the Agency and the State and its Officers, employees, agents and assigns harmless from any liability relating to personal injury or injury to real or tangible personal property of any kind, accruing or resulting to any other person, firm or corporation furnishing or supplying work, Services, materials or supplies in connection with the performance of this Contract, whether tangible or intangible,

arising out of the ordinary negligence, willful or wanton negligence, or intentional acts of the Vendor, its officers, employees, agents, assigns or subcontractors.

- c) Vendor shall not be liable for damages arising out of or caused by an alteration or an attachment not made or installed by the Vendor.
- 9) **MODIFICATION OF SERVICES:** If Vendor modifies or replaces the Services provided to the State and other tenants, and if the State has paid all applicable Subscription Fees, the State shall be entitled to receive, at no additional charge, access to a newer version of the Services that supports substantially the same functionality as the then accessible version of the Services. Newer versions of the Services containing substantially increased functionality may be made available to the State for an additional subscription fee. In the event of either of such modifications, the then accessible version of the Services shall remain fully available to the State until the newer version is provided to the State and accepted. If a modification materially affects the functionality of the Services as used by the State, the State, at its sole option, may defer such modification.
- 10) **TRANSITION PERIOD:**
 - a) For ninety (90) days, either prior to the expiration date of this Agreement, or upon notice of termination of this Agreement, Vendor shall assist the State, upon written request, in extracting and/or transitioning all Data in the format determined by the State ("Transition Period").
 - b) The Transition Period may be modified in an SLA or as agreed upon in writing by the parties in a contract amendment.
 - c) During the Transition Period, Services access shall continue to be made available to the State without alteration.
 - d) Vendor agrees to compensate the State for damages or losses the State incurs as a result of Vendor's failure to comply with this Transition Period section in accordance with the Limitation of Liability provisions above.
 - e) Upon termination, and unless otherwise stated in an SLA, and after providing the State Data to the State as indicated above in this section with acknowledged receipt by the State in writing, the Vendor shall permanently destroy or render inaccessible any portion of the State Data in Vendor's and/or subcontractor's possession or control following the completion and expiration of all obligations in this section. Within thirty (30) days, Vendor shall issue a written statement to the State confirming the destruction or inaccessibility of the State's Data.
 - f) The State at its option, may purchase additional Transition services as may be agreed upon in a supplemental agreement.
- 11) **TRANSPORTATION:** Transportation charges for any Deliverable sent to the State other than electronically or by download, shall be FOB Destination unless delivered by internet or file-transfer as agreed by the State, or otherwise specified in the solicitation document or purchase order.
- 12) **TRAVEL EXPENSES:** All travel expenses should be included in the Vendor's proposed costs. Separately stated travel expenses will not be reimbursed. In the event that the Vendor may be eligible to be reimbursed for travel expenses specifically agreed to in writing and arising under the performance of this Agreement, reimbursement will be at the out-of-state rates set forth in G.S. §138-6; as amended from time to time. Vendor agrees to use the lowest available airfare not requiring a weekend stay and to use the lowest available rate for rental vehicles. All Vendor incurred travel expenses shall be billed on a monthly basis, shall be supported by receipt and shall be paid by the State within thirty (30) days after invoice approval. Travel expenses exceeding the foregoing rates shall not be paid by the State. The State will reimburse travel allowances only for days on which the Vendor is required to be in North Carolina performing Services under this Agreement.
- 13) **PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES:** Vendor warrants that it has not paid, and agrees not to pay, any bonus, commission, fee, or gratuity to any employee or official of the State for the purpose of obtaining any contract or award issued by the State. Subsequent discovery by the State of non-compliance with these provisions shall constitute sufficient cause for immediate termination of all outstanding Agreements with the Vendor.

Violations of this provision may result in debarment of the Vendor(s) or Vendor(s) as permitted by 9 NCAC 06B.1207, or other provision of law.

- 14) **AVAILABILITY OF FUNDS:** Any and all payments by the State are expressly contingent upon and subject to the appropriation, allocation and availability of funds to the State for the purposes set forth in this Agreement. If this Agreement or any Purchase Order issued hereunder is funded in whole or in part by federal funds, the State's performance and payment shall be subject to and contingent upon the continuing availability of said federal funds for the purposes of the Agreement or Purchase Order. If the term of this Agreement extends into fiscal years subsequent to that in which it is approved such continuation of the Agreement *is expressly contingent upon* the appropriation, allocation, and availability of funds by the N.C. Legislature for the purposes set forth in the Agreement. If funds to effect payment are not available, the State will provide written notification to Vendor. If the Agreement is terminated under this paragraph, Vendor agrees to terminate any Services supplied to the State under this Agreement, and relieve the State of any further obligation thereof. The State shall remit payment for Services accepted on or prior to the date of the aforesaid notice in conformance with the payment terms.
- 15) **PAYMENT TERMS:**
- a) Payment may be made by the State in advance of or in anticipation of subscription Services to be actually performed under the Agreement or upon proper invoice for other Services rendered. Payment terms are Net 30 days after receipt of correct invoice. Initial payments are to be made after final acceptance of the Services. Payments are subject to any retainage requirements herein. The Purchasing State Agency is responsible for all payments under the Agreement. Subscription fees for term years after the initial year shall be as quoted under State options herein, but shall not increase more than 5% over the prior term, except as the parties may have agreed to an alternate formula to determine such increases in writing. No additional charges to the State will be permitted based upon, or arising from, the State's use of a Business Procurement Card. The State may exercise any and all rights of Set Off as permitted in Chapter 105A-4 *et seq.* of the N.C. General Statutes and applicable Administrative Rules.
 - b) Upon Vendor's written request of not less than 30 days and approval by the State, the State may:
 - i. Forward the Vendor's payment check(s) directly to any person or entity designated by the Vendor, or
 - ii. Include any person or entity designated in writing by Vendor as a joint payee on the Vendor's payment check(s), however,
 - iii. In no event shall such approval and action obligate the State to anyone other than the Vendor and the Vendor shall remain responsible for fulfillment of all Agreement obligations.
 - c) For any third party software licensed by Vendor or its subcontractors for use by the State, a copy of the software license including terms acceptable to the State, an assignment acceptable to the State, and documentation of license fees paid by the Vendor must be provided to the State before any related license fees or costs may be billed to the State.
 - d) An undisputed invoice is an invoice for which the State and/or the Purchasing State Agency has not disputed in writing within thirty (30) days from the invoice date, unless the agency requests more time for review of the invoice. Upon Vendor's receipt of a disputed invoice notice, Vendor will work to correct the applicable invoice error, provided that such dispute notice shall not relieve the State or the applicable Purchasing State Agency from its payment obligations for the undisputed items on the invoice or for any disputed items that are ultimately corrected. The Purchasing State Agency is not required to pay the Vendor for any Software or Services provided without a written purchase order from the appropriate Purchasing State Agency. In addition, all such Services provided must meet all terms, conditions, and specifications of this Agreement and purchase order and be accepted as satisfactory by the Purchasing State Agency before payment will be issued.
 - e) The Purchasing State Agency shall release any amounts held as retainages for Services completed within a reasonable period after the end of the period(s) or term(s) for which the retainage was withheld. Payment retainage shall apply to all invoiced items, excepting only

such items as Vendor obtains from Third Parties and for which costs are chargeable to the State by agreement of the Parties. The Purchasing State Agency, in its sole discretion, may release retainages withheld from any invoice upon acceptance of the Services identified or associated with such invoices.

16) ACCEPTANCE CRITERIA:

- a) Initial acceptance testing is required for all Vendor supplied Services before going live, unless provided otherwise in the solicitation documents or a Statement of Work. The State may define such processes and procedures as may be necessary or proper, in its opinion and discretion, to ensure compliance with the State's specifications and Vendor's technical representations. Acceptance of Services may be controlled by additional written terms as agreed by the parties.
- b) After initial acceptance of Services, the State shall have the obligation to notify Vendor, in writing and within ten (10) days following provision of any Deliverable described in the contract if it is not acceptable. The notice shall specify in reasonable detail the reason(s) a Deliverable is unacceptable. Acceptance by the State of any Vendor re-performance or correction shall not be unreasonably withheld, but may be conditioned or delayed as required for confirmation by the State that the issue(s) in the notice have been successfully corrected.

17) CONFIDENTIALITY: The State may maintain the confidentiality of certain types of information described in N.C. Gen. Stat. §132-1, *et seq.* Such information may include trade secrets defined by N.C. Gen. Stat. §66-152 and other information exempted from the Public Records Act pursuant to N.C. Gen. Stat. §132-1.2. Vendor may designate information, Products, Services or appropriate portions of its response as confidential, consistent with and to the extent permitted under the Statutes and Rules set forth above, by marking the top and bottom of pages containing confidential information with a legend in boldface type "**CONFIDENTIAL.**" By so marking any page, or portion of a page, the Vendor warrants that it has formed a good faith opinion, having received such necessary or proper review by counsel and other knowledgeable advisors, that the portions marked "confidential" meet the requirements of the Rules and Statutes set forth above. ***However, under no circumstances shall price information be designated as confidential.*** The State agrees to promptly notify the Vendor in writing of any action seeking to compel the disclosure of Vendor's confidential information. If an action is brought pursuant to N.C. Gen. Stat. §132-9 to compel the State to disclose information marked "confidential," the Vendor agrees that it will intervene in the action through its counsel and participate in defending the State, including any public official(s) or public employee(s). The Vendor agrees that it shall hold the State and any official(s) and individual(s) harmless from any and all damages, costs, and attorneys' fees awarded against the State in the action. The State shall have the right, at its option and expense, to participate in the defense of the action through its counsel. The State shall have no liability to Vendor with respect to the disclosure of Vendor's confidential information ordered by a court of competent jurisdiction pursuant to N.C. Gen. Stat. §132-9 or other applicable law.

18) SECURITY OF STATE DATA:

- a) All materials, including software, Data, information and documentation provided by the State to the Vendor (State Data) during the performance or provision of Services hereunder are the property of the State of North Carolina and must be kept secure and returned to the State. The Vendor will protect State Data in its hands from unauthorized disclosure, loss, damage, destruction by natural event, or other eventuality. Proprietary Vendor materials shall be identified to the State by Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be provided to the State as part of the Services. The Vendor shall not access State User accounts, or State Data, except (i) during data center operations, (ii) in response to service or technical issues, (iii) as required by the express terms of this contract, or (iv) at State's written request. The Vendor shall protect the confidentiality of all information, Data, instruments, studies, reports, records and other materials provided to it by the State or maintained or created in accordance with this Agreement. No such

information, Data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written agreement with the State. The Vendor will have written policies governing access to and duplication and dissemination of all such information, Data, instruments, studies, reports, records and other materials.

- b) The Vendor shall not store or transfer non-public State data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State of North Carolina data remotely only as required to provide technical support.
- c) Protection of personal privacy and sensitive data. The Vendor acknowledges its responsibility for securing any restricted or highly restricted data, as defined by the Statewide Data Classification and Handling Policy (<https://it.nc.gov/document/statewide-data-classification-and-handling-policy>) that is collected by the State and stored in any Vendor site or other Vendor housing systems including, but not limited to, computer systems, networks, servers, or databases, maintained by Vendor or its agents or subcontractors in connection with the provision of the Services. The Vendor warrants, at its sole cost and expense, that it shall implement processes and maintain the security of data classified as restricted or highly restricted; provide reasonable care and efforts to detect fraudulent activity involving the data; and promptly notify the State of any breaches of security within 24 hours of confirmation as required by N.C.G.S. § 143B-1379.
- d) The Vendor will provide and maintain secure backup of the State Data. The Vendor shall implement and maintain secure passwords for its online system providing the Services, as well as all appropriate administrative, physical, technical and procedural safeguards at all times during the term of this Agreement to secure such Data from Data Breach, protect the Data and the Services from loss, corruption, unauthorized disclosure, and the introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data and the Services. The Vendor will allow periodic back-up of State Data by the State to the State's infrastructure as the State requires or as may be provided by law.
- e) The Vendor shall certify to the State:
 - i. The sufficiency of its security standards, tools, technologies and procedures in providing Services under this Agreement;
 - ii. That the system used to provide the Subscription Services under this Contract has and will maintain a valid 3rd party security certification not to exceed 1 year and is consistent with the data classification level and a security controls appropriate for low or moderate information system(s) per the National Institute of Standards and Technology NIST 800-53 revision 4. The State reserves the right to independently evaluate, audit, and verify such requirements.
 - iii. That the Services will comply with the following:
 - (f) Any DIT security policy regarding Cloud Computing, and the DIT Statewide Information Security Policy Manual; to include encryption requirements as defined below:
 - (a) The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.
 - (b) For engagements where the Vendor stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. Examples are social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. The Vendor's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the Service Provider cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data

breach. Additionally, where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection;

- (2) Privacy provisions of the Federal Privacy Act of 1974;
 - (3) The North Carolina Identity Theft Protection Act, N.C.G.S. Chapter 75, Article 2A (e.g., N.C.G.S. § 75-65 and -66);
 - (4) The North Carolina Public Records Act, N.C.G.S. Chapter 132; and
 - (5) Applicable Federal, State and industry standards and guidelines including, but not limited to, relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines, Criminal Justice Information, The Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA);
 - (6) Any requirements implemented by the State under N.C.G.S. §§ 143B-1376 and -1377.
- f) **Security Breach.** "Security Breach" under the NC Identity Theft Protection Act (N.C.G.S. § 75-60ff) means (1) any circumstance pursuant to which applicable Law requires notification of such breach to be given to affected parties or other activity in response to such circumstance (e.g., N.C.G.S. § 75-65); or (2) any actual, attempted, suspected, threatened, or reasonably foreseeable circumstance that compromises, or could reasonably be expected to compromise, either Physical Security or Systems Security (as such terms are defined below) in a fashion that either does or could reasonably be expected to permit unauthorized Processing (as defined below), use, disclosure or acquisition of or access to any the State Data or state confidential information. "Physical Security" means physical security at any site or other location housing systems maintained by Vendor or its agents or subcontractors in connection with the Services. "Systems Security" means security of computer, electronic or telecommunications systems of any variety (including data bases, hardware, software, storage, switching and interconnection devices and mechanisms), and networks of which such systems are a part or communicate with, used directly or indirectly by Vendor or its agents or subcontractors in connection with the Services. "Processing" means any operation or set of operations performed upon the State Data or State confidential information, whether by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing or destroying.
- g) **Breach Notification.** In the event Vendor becomes aware of any Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall, at its own expense, (1) immediately notify the State's Agreement Administrator of such Security Breach and perform a root cause analysis thereon, (2) investigate such Security Breach, (3) provide a remediation plan, acceptable to the State, to address the Security Breach and prevent any further incidents, (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (5) cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach. The State shall make the final decision on notifying the State's persons, entities, employees, service providers and/or the public of such Security Breach, and the implementation of the remediation plan. If a notification to a customer is required under any Law or pursuant to any of the State's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by the State) shall be considered legally required.
- h) **Notification Related Costs.** Vendor shall reimburse the State for all Notification Related Costs incurred by the State arising out of or in connection with any such Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement resulting in a requirement for legally required notifications. "Notification Related Costs" shall include the State's internal and external costs associated with addressing and responding to the Security Breach, including but not limited to: (1) preparation and mailing or other transmission of legally required notifications; (2) preparation and mailing or other

transmission of such other communications to customers, agents or others as the State deems reasonably appropriate; (3) establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training); (4) public relations and other similar crisis management services; (5) legal and accounting fees and expenses associated with the State's investigation of and response to such event; and (6) costs for credit reporting services that are associated with legally required notifications or are advisable, in the State's opinion, under the circumstances. If the Vendor becomes aware of any Security Breach which is not due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall immediately notify the State of such Security Breach, and the parties shall reasonably cooperate regarding which of the foregoing or other activities may be appropriate under the circumstances, including any applicable Charges for the same.

- i) Vendor shall allow the State reasonable access to Services security logs, latency statistics, and other related Services security data that affect this Agreement and the State's Data, at no cost to the State.
- j) In the course of normal operations, it may become necessary for Vendor to copy or move Data to another storage destination on its online system, and delete the Data found in the original location. In any such event, the Vendor shall preserve and maintain the content and integrity of the Data, except by prior written notice to, and prior written approval by, the State.
- k) Remote access to Data from outside the continental United States, including, without limitation, remote access to Data by authorized Services support staff in identified support centers, is prohibited unless approved in advance by the State Chief Information Officer or the Using Agency.
- l) In the event of temporary loss of access to Services, Vendor shall promptly restore continuity of Services, restore Data in accordance with this Agreement and as may be set forth in an SLA, restore accessibility of Data and the Services to meet the performance requirements stated herein or in an SLA. As a result, Service Level remedies will become available to the State as provided herein, in the SLA or other agreed and relevant documents. Failure to promptly remedy any such temporary loss of access may result in the State exercising its options for assessing damages under this Agreement.
- m) In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to Data or Services, Vendor shall notify the State by the fastest means available and in writing, with additional notification provided to the State Chief Information Officer or designee of the contracting agency. Vendor shall provide such notification within twenty-four (24) hours after Vendor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Vendor shall inform the State of:
 - 1) The scale and quantity of the State Data loss;
 - 2) What Vendor has done or will do to recover the State Data from backups and mitigate any deleterious effect of the State Data and Services loss; and
 - 3) What corrective action Vendor has taken or will take to prevent future State Data and Services loss.
 - 4) If Vendor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Agreement.

Vendor shall investigate the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Vendor shall cooperate fully with the State, its agents and law enforcement.

- n) In the event of termination of this contract, cessation of business by the Vendor or other event preventing Vendor from continuing to provide the Services, Vendor shall not withhold the State Data or any other State confidential information or refuse for any reason, to promptly return to the State the State Data and any other State confidential information (including copies thereof) if requested to do so on such media as reasonably requested by the State, even if the State is then or is alleged to be in breach of the Agreement. As a part of Vendor's obligation to provide the State Data pursuant to this Paragraph 18) n),

Vendor will also provide the State any data maps, documentation, software, or other materials necessary, including, without limitation, handwritten notes, materials, working papers or documentation, for the State to use, translate, interpret, extract and convert the State Data.

- o) **Secure Data Disposal.** When requested by the State, the Vendor shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods and certificates of destruction shall be provided to the State.
- 19) **ACCESS TO PERSONS AND RECORDS:** Pursuant to N.C. General Statute 147-64.7, the State, the State Auditor, appropriate federal officials, and their respective authorized employees or agents are authorized to examine all books, records, and accounts of the Vendor insofar as they relate to transactions with any department, board, officer, commission, institution, or other agency of the State of North Carolina pursuant to the performance of this Agreement or to costs charged to this Agreement. The Vendor shall retain any such books, records, and accounts for a minimum of three (3) years after the completion of this Agreement. Additional audit or reporting requirements may be required by any State, if in the State's opinion, such requirement is imposed by federal or state law or regulation. The Vendor shall allow the State to audit conformance including contract terms, system security and data centers as appropriate. The State may perform this audit or contract with a third party at its discretion at the State's expense. Such reviews shall be conducted with at least 30 days' advance written notice and shall not unreasonably interfere with the Service Provider's business.
- 20) **ASSIGNMENT:** Vendor may not assign this Agreement or its obligations hereunder except as permitted by 09 NCAC 06B.1003 and this Paragraph. Vendor shall provide reasonable notice of not less than thirty (30) days of any consolidation, acquisition, or merger. Any assignee shall affirm this Agreement attorning to the terms and conditions agreed, and that Vendor shall affirm that the assignee is fully capable of performing all obligations of Vendor under this Agreement. An assignment may be made, if at all, in writing by the Vendor, Assignee and the State setting forth the foregoing obligation of Vendor and Assignee.
- 21) **NOTICES:** Any notices required under this Agreement should be delivered to the Agreement Administrator for each party. Unless otherwise specified in the Solicitation Documents, any notices shall be delivered in writing by U.S. Mail, Commercial Courier, facsimile or by hand.
- 22) **TITLES AND HEADINGS:** Titles and Headings in this Agreement are used for convenience only and do not define, limit or proscribe the language of terms identified by such Titles and Headings.
- 23) **AMENDMENT:** This Agreement may not be amended orally or by performance. Any amendment must be made in written form and signed by duly authorized representatives of the State and Vendor.
- 24) **TAXES:** The State of North Carolina is exempt from Federal excise taxes and no payment will be made for any personal property taxes levied on the Vendor or for any taxes levied on employee wages. Agencies of the State may have additional exemptions or exclusions for federal or state taxes. Evidence of such additional exemptions or exclusions may be provided to Vendor by Agencies, as applicable, during the term of this Agreement. Applicable State or local sales taxes shall be invoiced as a separate item.
- 25) **GOVERNING LAWS, JURISDICTION, AND VENUE:** This Agreement is made under and shall be governed and construed in accordance with the laws of the State of North Carolina. The place of this Agreement or purchase order, its situs and forum, shall be Wake County, North Carolina, where all matters, whether sounding in contract or in tort, relating to its validity, construction, interpretation and enforcement shall be determined. Vendor agrees and submits, solely for matters relating to this Agreement, to the jurisdiction of the courts of the State of North Carolina, and stipulates that Wake County shall be the proper venue for all matters.
- 26) **DEFAULT:** In the event Services or other Deliverable furnished or performed by the Vendor during performance of any Contract term fail to conform to any material requirement(s) of the Contract specifications, notice of the failure is provided by the State and if the failure is not cured within ten (10) days, or Vendor fails to meet the material requirements and specifications herein, the State may cancel the contract. Default may be cause for debarment as provided in

09 NCAC 06B.1206. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.

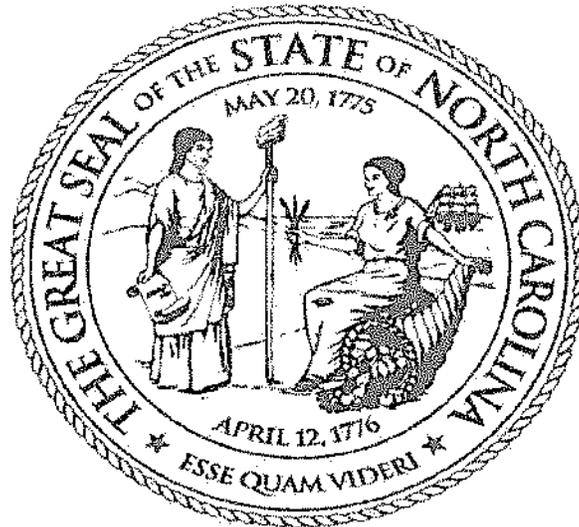
- a) If Vendor fails to deliver or provide correct Services within the time required by this Contract, the State shall provide written notice of said failure to Vendor, and by such notice require performance assurance measures pursuant to N.C.G.S. 143B-1340(f). Vendor is responsible for the delays resulting from its failure to deliver or provide Services as provided herein.
 - b) Should the State fail to perform any of its obligations upon which Vendor's performance is conditioned, Vendor shall not be in default for any delay, cost increase or other consequences resulting from the State's failure. Vendor will use reasonable efforts to mitigate delays, costs or expenses arising from assumptions in the Vendor's offer documents that prove erroneous or are otherwise invalid. Any deadline that is affected by any such Vendor failure in assumptions or performance by the State shall be extended by an amount of time reasonably necessary to compensate for the effect of such failure. Vendor shall provide a plan to cure any delay or default if requested by the State. The plan shall state the nature of the delay or default, the time required for cure, any mitigating factors causing or tending to cause the delay or default, and such other information as the Vendor may deem necessary or proper to provide.
- 27) **FORCE MAJEURE:** Except as provided for herein, neither party shall be deemed to be in default of its obligations hereunder if and so long as it is prevented from performing such obligations as a result of events beyond its reasonable control, including without limitation, fire, power failures, any act of war, hostile foreign action, nuclear explosion, riot, strikes or failures or refusals to perform under subcontracts, civil insurrection, earthquake, hurricane, tornado, or other catastrophic natural event or act of God.
- 28) **COMPLIANCE WITH LAWS:** The Vendor shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business and the provision of Services hereunder, including those of federal, state, and local agencies having jurisdiction and/or authority.
- 29) **TERMINATION:** Any notice or termination made under this Agreement shall be transmitted via US Mail, Certified Return Receipt Requested. The period of notice for termination shall begin on the day the return receipt is signed and dated. The parties may mutually terminate this Agreement by written agreement at any time.
- a) The State may terminate this Agreement, in whole or in part, pursuant to the Paragraph entitled "Default," above, or pursuant to Special Terms and Conditions in the Solicitation Documents, if any, or for any of the following
 - i) Termination for Cause: In the event any goods, Services, or service furnished by the Vendor during performance fails to conform to any material specification or requirement of the Agreement, and the failure is not cured within the specified time after providing written notice thereof to Vendor, the State may cancel and procure the articles or Services from other sources, holding Vendor liable for any excess costs occasioned thereby, subject only to the limitations provided in Paragraph 7), entitled "Limitation of Liability." The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Agreement. Vendor shall not be relieved of liability to the State for damages sustained by the State arising from Vendor's breach of this Agreement; and the State may, in its discretion, withhold any payment due as a setoff until such time as the damages are finally determined or as agreed by the parties. Voluntary or involuntary Bankruptcy or receivership by Vendor shall be cause for termination.
 - ii) Termination for Convenience Without Cause: The State may terminate service and indefinite quantity contracts, in whole or in part by giving thirty (30) days prior notice in writing to the Vendor. Vendor shall be entitled to sums due as compensation for Services performed in conformance with the Agreement. In the event the Agreement is terminated for the convenience of the State the State will pay for all Services and work performed or delivered in conformance with the Agreement up to the date of termination.

- 30) **DISPUTE RESOLUTION:** The parties agree that it is in their mutual interest to resolve disputes informally. A claim by the State shall be submitted in writing to the Vendor's Agreement Administrator for decision. The Parties shall negotiate in good faith and use all reasonable efforts to resolve such dispute(s). During the time the Parties are attempting to resolve any dispute, each shall proceed diligently to perform their respective duties and responsibilities under this Agreement. If a dispute cannot be resolved between the Parties within thirty (30) days after delivery of notice, either Party may elect to exercise any other remedies available under this Agreement, or at law. This term shall not constitute an agreement by either party to mediate or arbitrate any dispute.
- 31) **SEVERABILITY:** In the event that a court of competent jurisdiction holds that a provision or requirement of this Agreement violates any applicable law, each such provision or requirement shall be enforced only to the extent it is not in violation of law or is not otherwise unenforceable and all other provisions and requirements of this Agreement shall remain in full force and effect. All promises, requirements, terms, conditions, provisions, representations, guarantees and warranties contained herein shall survive the expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable federal or State statute, including statutes of repose or limitation.
- 32) **FEDERAL INTELLECTUAL PROPERTY BANKRUPTCY PROTECTION ACT:** The Parties agree that the State shall be entitled to any and all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto.
- 33) **ELECTRONIC PROCUREMENT:** (Applies to all contracts that include E-Procurement and are identified as such in the body of the solicitation document): Purchasing shall be conducted through the Statewide E-Procurement Service. The State's third party agent shall serve as the Supplier Manager for this E-Procurement Service. The Vendor shall register for the Statewide E-Procurement Service within two (2) business days of notification of award in order to receive an electronic purchase order resulting from award of this contract. The E-Procurement fee does not normally apply to services.
- a) Reserved.
 - b) Reserved.
 - c) The Supplier Manager will capture the order from the State approved user, including the shipping and payment information, and submit the order in accordance with the E-Procurement Service. Subsequently, the Supplier Manager will send those orders to the appropriate Vendor on State Agreement. The State or State approved user, not the Supplier Manager, shall be responsible for the solicitation, bids received, evaluation of bids received, award of contract, and the payment for goods delivered.
 - d) Vendor agrees at all times to maintain the confidentiality of its user name and password for the Statewide E-Procurement Services. If a Vendor is a corporation, partnership or other legal entity, then the Vendor may authorize its employees to use its password. Vendor shall be responsible for all activity and all charges for such employees. Vendor agrees not to permit a third party to use the Statewide E-Procurement Services through its account. If there is a breach of security through the Vendor's account, Vendor shall immediately change its password and notify the Supplier Manager of the security breach by e-mail. Vendor shall cooperate with the state and the Supplier Manager to mitigate and correct any security breach.

Vendor Readiness Assessment Report

Attachment B. ENTERPRISE SECURITY & RISK
MANAGEMENT OFFICE (ESRMO) VENDOR ASSESSMENT
GUIDE

ENTERPRISE SECURITY & RISK
MANAGEMENT OFFICE (ESRMO)



Vendor Readiness Assessment Report (VRR)

Executive Summary

The State requires that all systems connected to the State network or process State data, meet an acceptable level of security compliance. This includes those systems that operate outside of the States' direct control such as Cloud Services defined as Software as a Service (SaaS), Infrastructure as a Service (IaaS) or Platform as a Service (PaaS). Below is a high level view of specific security requirements that are requirements to meet compliance. Note: There may be additional requirements depending on the sensitivity of the data and other Federal and State mandates

Introduction

Purpose

This report and its underlying assessment are intended to enable State agencies to reach a state-ready decision for a specific Cloud Service Provider's system based on organizational processes and the security capabilities of the Moderate/low-impact information system. The "**Outcome**" and the "**State Approach and Use of This Document**" sections below indicate how this document will impact this solicitation process.

- **Outcomes**

Submission of this report by the Vendor does not guarantee a state-ready designation, nor does it guarantee that the state will procure services from the vendor.

- **State Approach and Use of This Document**

The VRAR identifies clear and objective State security capability requirements, where possible, while also allowing for the presentation of more subjective information. The clear and objective requirements enable the Vendor to concisely identify whether an application or vendor is achieving the most important State Moderate or low baseline requirements. The combination of objective requirements and subjective information enables State to render a readiness decision based on a more complete understanding of the vendor's security capabilities. Again, submission of this report by the Vendor does not guarantee a state-ready designation, nor does it guarantee that the state will procure services from the vendor.

Section 4, Capability Readiness, is organized into three sections:

- **Section 4.1, State Mandates**, identifies a small set of the state mandates a vendor must satisfy. State **will not** waive any of these requirements.
- **Section 4.2, State Requirements**, identifies an excerpt of the most compelling

requirements from the National Institute of Science and Technology (NIST) Special Publication (SP) 800 document series and State guidance. A VENDOR is unlikely to achieve approval if any of these requirements are not met.

- **Section 4.3, Additional Capability Information**, identifies additional information that is not tied to specific requirements, yet has typically reflected strongly on a VENDOR's ability to achieve approval.

VENDOR System Information

Provide and validate the information below. For example, if the deployment model is Government only, ensure there are no non-Government customers. The VRAR template is intended for systems categorized at the Moderate security impact level, in accordance with the FIPS Publication 199 Security Categorization.

Table 3-1. System Information

<p>VENDOR Name: Carahsoft and DocuSign System Name: DocuSign Service Model: SaaS FIPS PUB 199 System Security Level: (Moderate) Fully Operational as of: 2003 Number of Customers (State/Others): 400,000+ Deployment Model: Government Cloud System Functionality: DocuSign is an electronic signature and workflow management application hosted in a datacenter. Customers determine and manage the documents and workflow used in their instance of</p>

Relationship to Other Vendors or CSPs

If this Moderate baseline system resides in another VENDOR's environment or inherits security capabilities, please provide the relevant details in Tables 3-2 and 3-3 below. Please note, the leveraged system itself must be State Authorized. For example, a large VENDOR may have a commercial service offering and a separate service offering with a State Authorization. Only the service offering with the State Authorization may be leveraged.

IMPORTANT: If there is a leveraged system, be sure to note every capability in Section 4 that partially or fully leverages the underlying system. When doing so, indicate the capability is fully inherited or describe both the inherited and non-inherited aspects of the capability.

Table 3-2. Leveraged Systems

#	Question	Yes	No	N/A	If Yes, please describe.
1	Is this system leveraging an underlying provider?	X			DocuSign leases datacenter space (ping, pipe, power) from various facilities. Datacenters are PCI DSS

				<p>compliant and SSAE examined by their own auditors.</p> <p>DocuSign owns the hardware, software (or software licenses where applicable) and applications (application licenses where applicable) within the leased datacenter space.</p> <p>DocuSign hosts the application on DocuSign owned equipment within the leased datacenter space.</p>
--	--	--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

List all **services** leveraged. The system from which the service is leveraged must be listed in Table 3-2 above.

Table 3-3. Leveraged Services

#	Service	Service Capability	System
1	<p><i>Cyxtera</i></p> <p><i>SunGard</i></p> <p><i>Equinix</i></p>	<p>DocuSign leases datacenter space (ping, pipe, power) from various facilities. Datacenters are PCI DSS compliant and SSAE examined by their own auditors.</p> <p>DocuSign owns the hardware, software (or software licenses where applicable) and applications (application licenses where applicable) within the leased datacenter space.</p> <p>DocuSign hosts the application on DocuSign owned equipment within the leased datacenter space.</p>	<p>DocuSign Federal is hosted in four (4) co-location datacenter facilities within the continental United States specifically chosen due to their adherence to industry-standard physical security and availability protections. These datacenter facilities are located in Chicago, Illinois; Seattle, Washington; and Richardson, Texas. The facilities are managed by Cyxtera (Chicago and Seattle), SunGard (Richardson), and Equinix (Chicago) and meet common industry security control requirements, including SSAE16 and FISMA controls. DocuSign Federal is housed within heavily access-restricted datacenter cages within each facility, with multiple layers of physical access control, authentication, and</p>

#	Service	Service Capability	System
			authorization before personnel or information system components are permitted access. Further, DocuSign Federal has dedicated multi-tenant security appliances and network area storage units to segregate Federal Agency data from other DocuSign customers. In addition to the datacenter facilities, certain ancillary DocuSign Federal components are hosted within AWS, Azure, and Akamai. These components are logically integrated with the network boundary present in the datacenter facilities.

Data Flow Diagrams

- *Please see DocuSign Security and Trust Assurance Packet for Data Flow Diagrams*
- *clearly identify data flows for privileged, non-privileged and customers access; and*
- *depict how all ports, protocols, and services of all inbound and outbound traffic are represented and managed.*

Separation Measures [AC-4, SC-7]

Assess and describe the strength of the physical and/or logical separation measures in place to provide segmentation and isolation of tenants, administration, and operations; addressing user-to-system; admin-to-system; and system-to-system relationships.

The Vendor must base the assessment of separation measures on very strong evidence, such as the review of any existing penetration testing results, or an expert review of the products, architecture, and configurations involved. The Vendor must describe how the methods used to verify the strength of separation measures.

System Interconnections

A System Interconnection is a dedicated connection between information systems, such as between a SaaS/PaaS and underlying IaaS.

The Vendor must complete the table below. If the answer to any question is "yes," please briefly describe the connection. Also, if the answer to the last question is "yes," please complete Table 3-4 below.

Table 3-3. System Interconnections

#	Question	Yes	No	If Yes, please describe.
1	Does the system connect to the Internet?	X		DocuSign is an electronic signature and workflow management application hosted in a datacenter. Customers determine and manage the documents and workflow used in their instance of DocuSign. DocuSign enables customers to directly upload documents for signature over secure sessions where the customer documents are systematically encrypted. DocuSign personnel do not have access to customer documents.
2	Does the system connect to a corporate or state infrastructure/network?		X	
4	Does the system connect to external systems?		X	If "yes," complete Table 3-4 below.

If there are connections to external systems, please list each in the table below, using one row per interconnection. If

there are no external system connections, please type "None" in the first row.

Table 3-4. Interconnection Security Agreements (ISAs)

#	External System Connection	Does an ISA Exist?		Interconnection Description. If no ISA, please justify below.
		Yes	No	
1	None			
2				

Capability Readiness

State Mandates

This section identifies State requirements applicable to all State approved systems. All requirements in this section must be met. Some of these topics are also covered in greater detail in Section o, *State Requirements*, below.

Only answer "Yes" if the requirement is fully and strictly met. The Vendor must answer "No" if an alternative implementation is in place.

Table 4-1. State Mandates

#	Compliance Topic	Fully Compliant?	
		Yes	No
1	Are FIPS 140-2 Validated or National Security Agency (NSA)-Approved cryptographic modules consistently used where cryptography is required? Only True with FedRAMP offering	X	

#	Compliance Topic	Fully Compliant?	
		Yes	No
2	<p>What type of authentication does the application use? Can it integrate with the State's NCID solution?</p> <p>Only true if SSO is enabled (Which comes with the FedRAMP offering</p> <p>Our implementation offers highly configurable customer options for authentication of users and signers. Users can authenticate within the HTTPS web browser using their DocuSign System username and password or through one of the several external authentication mechanisms offered including SAML. DocuSign users determine the level and number of authentication layers for the signer. Senders can choose from options to require an access code establish identity, or DocuSign's two-factor biometric authentication offering called Phone Authentication.</p>	X	
3	<p>What types of security boundary/threat protection devices are used to protect the network, system, application...e.g. firewalls intrusion detection/prevention systems, end point protection etc.</p> <p>DocuSign employs a defense in-depth strategy which includes F5, Cisco, Juniper, and Snort network devices. In addition, DocuSign has anti-virus protection including McAfee and CarbonBlack on endpoint devices.</p> <p>DocuSign utilizes commercial grade security software and hardware to protect our eSignature service. DocuSign implements a defense-in-depth approach to hardening our production environment against exposure and attack. Isolated, commercial grade network management controls in production include dedicated load balancers, firewalls, intrusion detection system (IDS) distributed across production networks, and malware protections.</p>	X	
4	<p>Does the VENDOR have the ability to consistently remediate High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days?</p> <p>Only True with FedRAMP Offering</p> <p>Critical: Immediate</p> <p>High: 30 days</p> <p>Medium: 90 days</p>	X	
5	<p>Does the VENDOR and system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements?</p>		X Not explicitly controlled by those requirements, however document

#	Compliance Topic	Fully Compliant?	
		Yes	No
			t manage ment and retention is managed by the customer

State Requirements

This section identifies additional State Readiness requirements. All requirements in this section must be met; however, alternative implementations and non-applicability justifications may be considered on a limited basis.

Approved Cryptographic Modules [SC-13]

The Vendor must ensure FIPS 140-2 Validated or NSA-Approved algorithms are used for all encryption modules. FIPS 140-2 Compliant is not sufficient. The Vendor may add rows to the table if appropriate, but must not remove the original rows. The Vendor must identify all non-compliant cryptographic modules in use.

Table 4-2. Cryptographic Modules

	Cryptographic Module Type	FIPS 140-2 Validated?		NSA Approved?		Describe Any Alternative Implementations (if applicable)	Describe Missing Elements or N/A Justification
		Yes	No	Yes	No		
1	Data at Rest [SC-28]	X			X	DocuSign encrypts Federal Agency data and documents in DocuSign Federal by using the FIPS 140-2 validated Microsoft Crypto API with AES 256 encryption before storing such documents within the respective Blobs and NAS(s). DocuSign has deployed MTSA's in DocuSign Federal, which store and control the document	

	Cryptographic Module Type	FIPS 140-2 Validated?		NSA Approved?		Describe Any Alternative Implementations (if applicable)	Describe Missing Elements or N/A Justification
		Yes	No	Yes	No		
						<p>encryption keys used by Federal Agency users. The MTSA's are in-house built key store solutions that are access controlled and segregated to only Federal Agencies. Additionally, DocuSign Federal provides Federal Agencies the ability to deploy MTSA's and storage via on-premises solutions if they require segregation from other Federal Agency data. Furthermore, DocuSign uses the MTSA's with Thales PCI-based HSM's to generate the AES-256 symmetric keys. The HSM's are rated at FIPS 140-2 Level 3 which provides stronger cryptographic operations to encrypt the BLOB files.</p>	
2	Transmission [SC-8 (1), SC-12, SC-12(2, 3)]	X			X	DocuSign has implemented federally approved cryptography within DocuSign Federal in accordance with applicable Federal	

Cryptographic Module Type	FIPS 140-2 Validated?		NSA Approved?		Describe Any Alternative Implementations (if applicable)	Describe Missing Elements or N/A Justification
	Yes	No	Yes	No		
					<p>Laws, Executive Orders, directives, policies, regulations, and standards. For example, all access to the production environment is encrypted, whether TLS for customer connections to the front-end webservers, (see SC-8 for more information), or administrative remote access through a TLS VPN connection (see AC-17 and IA-2 for more information).</p> <p>DocuSign also uses MTSA's with Thales PCI-based HSM's to generate AES-256 symmetric keys, a solution rated at FIPS 140-2 Level 3.</p> <p>DocuSign relies on Symantec Corporation, a third-party trusted CA, for external SSL certificates. All SSL certificates are RSA 2048-bit certificates. The SSL certificates are controlled using DocuSign Federal load balancers, which are heavily access controlled in accordance with AC-4 and SC-7, to create TLS connections that authenticate and encrypt Federal Agency data.</p>	

	Cryptographic Module Type	FIPS 140-2 Validated?		NSA Approved?		Describe Any Alternative Implementations (if applicable)	Describe Missing Elements or N/A Justification
		Yes	No	Yes	No		
3	Remote Access [AC-17 (2)]	N/A	N/A				
4	Authentication [IA-5 (1), IA-7]	X			X	<p>DocuSign CORP Accounts: DocuSign requires Technical Operations personnel who need access to DocuSign Federal system boundary to have HQ AD domain usernames and approval from the CTO or Vice President of Technical Operations of their Authorization – Access to Production Environment change request. Technical Operations creates new CORP AD domain usernames based on their HQ AD domain usernames and configures a temporary password in accordance with the password requirements in IA-5(1). During the initial log-on, the temporary passwords must be changed immediately to a password that meets password requirements defined in IA-5(1).</p> <p>Only after receiving a CORP AD account are authorized Technical Operations employees permitted to obtain additional authenticators, including Dell Defender authenticator tokens, local device accounts, or local application administration accounts. These local accounts are</p>	

Cryptographic Module Type	FIPS 140-2 Validated?		NSA Approved?		Describe Any Alternative Implementations (If applicable)	Describe Missing Elements or N/A Justification
	Yes	No	Yes	No		
					<p>provisioned for network devices, Linux components, application administrative portal, and AWS, Azure, Akamai enterprise account management functions.</p> <p>DocuSign Jump Host Accounts: DocuSign requires Technical Operations personnel who need access to DocuSign Federal system boundary to have HQ AD domain usernames and approval from the CTO or Vice President of Technical Operations of their Authorization – Access to Production Environment change request. Technical Operations creates new Jump Host AD domain usernames based on their HQ AD domain usernames and configures a temporary password in accordance with the password requirements in IA-5(1). During the initial log-on, the temporary passwords must be changed immediately to a password that meets password requirements defined in IA-5(1).</p> <p>DocuSign Administrator Accounts: DocuSign requires personnel who want access to application</p>	

	Cryptographic Module Type	FIPS 140-2 Validated?		NSA Approved?		Describe Any Alternative Implementations (if applicable)	Describe Missing Elements or N/A Justification
		Yes	No	Yes	No		
						<p>administrator console to have HQ AD domain usernames and approval from both their direct manager and Technical Operations of their Authorization – Admin Console Access. Technical Operations sends activation emails to their DocuSign email addresses.</p> <p>Federal Agency Accounts: Federal agencies follow their own policies. For more information on Federal Agency user accounts, refer to IA-8 and a description of how a Federal Agency can integrate their existing account management and authentication infrastructure using the SAML SSO functionality of DocuSign Federal.</p>	
5	Digital Signatures/Hash [CM-5 (3)]	X			X	<p>Authorized Technical Operations members are reviewed, approved, and provisioned access to DocuSign Federal in accordance with AC-2, AC-3, and AC-5. System access is granted based on intended system usage, valid system access authorization and physical access, and responsibilities for mission/business</p>	

	Cryptographic Module Type	FIPS 140-2 Validated?		NSA Approved?		Describe Any Alternative Implementations (if applicable)	Describe Missing Elements or N/A Justification
		Yes	No	Yes	No		
						functions. All Technical Operations members authorized to access DocuSign Federal are managed, identified, and authenticated in a consistent fashion in accordance with AC-2, IA-2, and IA-2(1).	

Transport Layer Security [NIST SP 800-52, Revision 1]

The Vendor must identify all protocols in use. The Vendor may add rows to the table if appropriate, but must not remove the original rows.

Table 4-3. Transport Layer Security

#	The Cryptographic Module Type	Protocol In Use?		If "yes," please describe use for both internal and external communications
		Yes	No	
1.	SSL (Non-Compliant)		X	
2	TLS 1.0 (Non-Compliant)		X	Some customers have not been able to migrate from TLS 1.0 due to legacy applications. In these cases, customers must sign an agreement to assume the risk of continuing to use TLS 1.0.
3	TLS 1.1 (Compliant)	X		DocuSign's production email service utilizes both DKIM for signing outbound email and TLS to assure confidential communication occurs over an encrypted session.
4	TLS 1.2 (Compliant)	X		

Identification and Authentication, Authorization, and Access Control

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Table 4-4. Identification and Authentication, Authorization, and Access Control

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
2	Does the system uniquely identify and authorize organizational users (or processes acting on behalf of organizational users) in a manner that cannot be repudiated and which sufficiently reduces the risk of impersonation? [IA-2, IA-4, IA-4(4)]	X		<p>DocuSign HQ Accounts: All DocuSign personnel are authorized to access the DocuSign HQ environment and standard corporate resources. All DocuSign personnel are provisioned a DocuSign HQ domain account, which is used to access their workstation and DocuSign corporate resources; DocuSign HQ domain accounts are stored within the corporate Active Directory, which is managed by Corporate IT in accordance with corporate account management procedures, as well as the onboarding, termination, and transfer processes described in PS-3, PS-4, and PS-5. DocuSign HQ domain accounts have no access to DocuSign Federal and are considered out of scope of the DocuSign Federal authorization boundary. But, DocuSign personnel with DocuSign CORP or Application Administration accounts are required to be on the corporate network, which requires DocuSign HQ credentials, to access the VPN or web application.</p> <p>DocuSign CORP Accounts: All DocuSign personnel requiring access to DocuSign Federal or system components are provisioned a DocuSign CORP domain account and/or local accounts. DocuSign CORP domain accounts are stored within the back-end, production environment Active Directory, which is managed by Technical Operations administrators. All DocuSign Technical Operations, Security Operations, and Product Security personnel authorized to access DocuSign Federal are considered privileged users and are managed, identified, and authenticated in a consistent fashion in accordance with AC-3 and IA-2.</p> <p>DocuSign establishes two different CORP AD domain account types for DocuSign Federal: front-end domain accounts and back-end domain accounts. Both front-end domain accounts and back-end domain accounts provide users domain access to either front-end components or back-end components, respectively. DocuSign restricts provisioning of these CORP AD</p>

SOLICITATION # ITS-400335

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				<p>domain accounts to only Technical Operations personnel to perform their designated roles and responsibilities of managing DocuSign Federal. DocuSign approves a limited amount Technical Operations administrators as domain account managers.</p> <p>DocuSign Technical Operations personnel uniquely identify and authenticate to DocuSign Federal by connecting to the system's VPN, providing their Dell Defender MFA token and back-end domain account credentials. Once connected to the VPN, DocuSign Technical Operations personnel connect either to the RDP gateway or SSH jump host by uniquely identifying and authenticating with a separate Dell Defender MFA token for Windows-based hosts or SSH keys for Linux-based hosts. Once connected to either the RDP gateway or SSH jump host, DocuSign Technical Operations personnel connect to a Windows-based host or Linux-based host tied to CORP AD by authenticating with their front-end or back-end credentials, depending on the location of the host within DocuSign Federal.</p> <p>DocuSign uses local accounts for network devices and hardware components within DocuSign Federal that are not integrated into the DocuSign CORP AD. In order to authenticate to these local device accounts, users must connect via the SSH jump host using their SSH keys and local device account credentials. In addition, DocuSign uses local accounts for AWS EC2 Linux-based servers, which are only accessible via the jump hosts within DocuSign Federal. For connecting to AWS VPC hosts, DocuSign Technical Operations personnel connect to the AWS VPCs by connecting to DocuSign Federal VPN then connecting via the SSH jump host using their SSH keys and local host account credentials.</p> <p>DocuSign Jump Host Accounts: The jump host domain account provides user access to the back-end jump host, which provides users the ability to RDP or</p>

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				<p>SSH to front-end or back-end components. DocuSign restricts provisioning of these CORP AD domain accounts to only Technical Operations personnel to perform their designated roles and responsibilities of managing DocuSign Federal. DocuSign approves a limited amount Technical Operations administrators as domain account managers.</p> <p>DocuSign Technical Operations personnel uniquely identify and authenticate to DocuSign Federal by connecting to the system's VPN, providing their Dell Defender MFA token and back-end domain account credentials. Once connected to the VPN, DocuSign Technical Operations personnel connect either to the RDP gateway or SSH jump host by uniquely identifying and authenticating with a separate Dell Defender MFA token for Windows-based hosts or SSH keys for Linux-based hosts.</p> <p>AWS, Azure, Akamai Accounts: DocuSign Federal uses local accounts to access the AWS, Azure, and Akamai management consoles that are used for deploying and decommissioning system components within those locations. The AWS, Azure, and Akamai management console accounts are managed by the enterprise account owners within Technical Operations using the respective vendor's enterprise account management functionality.</p> <p>DocuSign Administrator Accounts: DocuSign Federal Account Management Support uses local, privileged accounts to authenticate to certain limited account support functions within the internal application account administrative web interface. These limited functions are used by account support personnel in the execution of their job responsibilities to fulfill Federal Agency account management functions, such as enabling features. The DocuSign Federal internal application account administrative web interface is only reachable from the DocuSign network. DocuSign restricts provisioning of these local</p>

SOLICITATION # ITS-400335

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				accounts to only Technical Operations personnel to perform their designated roles and responsibilities of managing DocuSign Federal.

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
3	Does the system require multi-factor authentication (MFA) for administrative accounts and functions? [IA-2, IA-2(1), IA-2(3)]		X	MFA is not required, however can be configured within DocuSign and Customer SSO
4	Does the system fully comply with eAuth Level 3 or higher? [NIST SP 800-63]	X		Since SSO must be enabled to interface with NCID, state agencies are responsible for this requirement by enforcing a second factor authentication method.
5	Does the system restrict non-authorized personnel's access to resources? [AC-6(2)]	X		
6	Does the system restrict non-privileged users from performing privileged function? [AC-6(10)]	X		
7	Does the system ensure secure separation of customer data? [SC-4]	X		DocuSign is committed to the highest levels of service and protection. DocuSign uses a multi-tenant architecture. All customer confidential envelope content including documents, signatures and document form data are stored in AES encrypted fashion. All Envelope and encrypted document data is keyed to customer account and sending account identity using account and user unique identifiers. All documents and other sensitive customer data are stored in an encrypted fashion in a secure datacenter which is physically segregated from DocuSign's corporate networks.
8	Does the system ensure secure separation of customer processing environments? [SC-2, SC-3]	X		See above

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
9	Does the system restrict access of administrative personnel in a way that limits the capability of individuals to compromise the security of the information system? [AC-2(7)]	X		
10	Does the remote access capability include VENDOR-defined and implemented usage restrictions, configuration guidance, and authorization procedure? [AC-17]	N/A	N/A	Remote access not a product feature. DocuSign is an electronic signature and workflow management application hosted in a datacenter. Customers determine and manage the documents and workflow used in their instance of DocuSign. DocuSign enables customers to directly upload documents for signature over secure sessions where the customer documents are systematically encrypted. DocuSign personnel do not have access to customer documents.

Audit, Alerting, Malware, and Incident Response

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Table 4-5. Audit, Alerting, Malware, and Incident Response

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the system have the capability to detect, contain, and eradicate malicious software? [SI-3, SI-3 (1), SI-3 (2), SI-3 (7), MA-3 (2)]	X		DocuSign maintains commercially available, enterprise class, antivirus/antimalware software and performs routine infrastructure and application vulnerability scanning. Antivirus signatures are automatic and performed daily. Users do not have either ability to disable those controls or alter the configuration. As a PCI DSS compliant level 1 service provider/ level 3 merchant, DocuSign performs internal monthly vulnerability scanning and quarterly application scanning at a minimum. Quarterly external scans are conducted by a qualified third party and annual penetration testing is conducted against both the DocuSign application and its infrastructure by credentialed, industry recognized organizations. DocuSign maintains a formal SDLC and related programs, such as Patch

SOLICITATION # ITS-400335

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				Management, which are ISO27001, PCI DSS, and SSAE16 examined and certified Patches are obtained from vendors and deployed on a monthly basis across all production environments and network vulnerability scans are conducted afterward. Emergency patches are immediately applied as needed and follow Change Management procedures. The following is the patch categories: Critical: Immediate High: 30 days Medium: 90 days
2	Does the system store audit data in a tamper-resistant manner which meets chain of custody and any e-discovery requirements? [AU-7, AU-9]	X		DocuSign has a logging, monitoring deployment that captures and correlates log events in real-time from systems and devices to both Operations and Security. Operations and Security personnel have access to the logs, but logs cannot be modified, substituted, or deleted by said personnel. Logs are stored within a SQL database which is used as a data store by the application. Logs are securely written to the database. Access to the SQL data stores is tightly restricted.

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
3	Does the VENDOR have the capability to detect unauthorized or malicious use of the system, including insider threat and external intrusions? [SI-4, SI-4 (4), SI-7, SI-7 (7)]	X		DocuSign uses a McAfee ELM to capture logs from DocuSign Federal production components. The McAfee SIEM produces alerts based off of the logs from the ELM. Houston, an in-house DocuSign tool, forwards those alerts to the Redmine ISCM to automatically generate cases to be analyzed by the CSIRT team, to ensure the system components are functioning in an optimal, resilient, and secure state. CSIRT monitors the automatically generated ISCM cases for unauthorized access to and use of DocuSign Federal in accordance with AU-2. CSIRT uses a SIEM solution to capture and correlate all application logs from system components and tools within DocuSign Federal. All Windows and CentOS servers send system event logs to the SIEM. Additionally, FIM (OSSEC), ClamAV, SCEP, and SNORT IDS forward system event logs

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				<p>to the SIEM.</p> <p>DocuSign has also built an in-house performance monitoring solution, KazMon, which deploys local custom agents to monitor performance and events related to the system components and web applications within DocuSign Federal. These logs are not forwarded to the SIEM, but are centrally managed via the in-house built KazMon solution. Additionally, KazMon monitors for any changes against the baseline OS configurations.</p> <p>The SIEM uses the ELM to manage logs in a read-only mode and retain logs for one (1) year. DocuSign limits access to the SIEM, ELM, and audit infrastructure to authorized CSIRT and Information Security members, in accordance to AC and IA control families, to protect the information obtained during monitoring.</p> <p>CSIRT heightens monitoring activities as necessary due to vulnerabilities or suspicious activities are uncovered within DocuSign Federal. In addition, CSIRT heightens monitoring activities when there are alerts from external sources which includes Technical Security Alerts and Security Bulletins from US-CERT as well advisories from FedRAMP. CSIRT can create dashboards or other visualizations in the SIEM to track specific events, specific platforms, or combinations thereof.</p> <p>DocuSign obtains legal opinions with regard to monitoring as necessary. In accordance with AC-8, DocuSign notifies all users accessing DocuSign Federal about monitoring. Further, DocuSign obtains users' consent of such monitoring as a requirement in order to access the system.</p> <p>For events that meet the pattern of a known attack methodology, CSIRT track and document validated security incidents as new cases within ISCM. CSIRT follows the Incident Response Playbook to resolve the incident and notifies the applicable DocuSign Federal stakeholders as needed.</p>
4	Does the VENDOR have an Incident Response Plan and a fully developed Incident Response test plan? [IR-3, IR-8]	X		All DocuSign personnel involved in Information System Incident Response activities must participate in an annual

SOLICITATION # ITS-400335

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				<p>incident response testing exercise. The annual testing is conducted as a tabletop exercise to measure the effectiveness and document lessons learned. Annual testing is treated as both a learning and training exercise for personnel associated with handling incident response activities. The exact security incident to be tested will be at the discretion of the CISO in accordance with NIST SP 800-61.</p>
5	<p>Does the VENDOR have a plan and capability to perform security code analysis and assess code for security flaws, as well as identify, track and remediate security flaws? [SA-11, SA-11 (1), SA-11 (8)]</p>	X		<p><i>DocuSign software developers follow a security assessment plan when developing code. The purpose of this sort of plan is to integrate security measures with developing code. Security control incorporation requires testing to ensure that, like any other piece of code that is included in software, no vulnerability is inadvertently introduced. The plan includes both coverage and depth of code testing. Testing can take the forms of static code analysis and of dynamic code analysis. DocuSign software developers adhere to a security plan when developing code, and leverage both static and dynamic code analysis and tools such as regression testing.</i></p> <p><i>Once the developer has completed the change, the developer tests the specific change in a remote sandbox environment within Azure called OneBox until the change passes all local automated tests and is ready for acceptance testing. At this time, the developer conducts unit testing before any source code changes are integrated back into the source code tree. During this cycle, the developer may integrate several times with the central repository master branch, which gets pushed automatically to the development integration server where developers perform further testing.</i></p> <p><i>After successful testing by the</i></p>

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				<p><i>developer, the changes are peer reviewed by another developer in Engineering. Once reviewed, the changes are integrated into the release branch. Then, the release branch is pushed to the QA testing environment where QA performs integration and system testing using DocuSign's internally developed Sawmill tool. Then, the release branch is pushed into a staging environment where QA performs regression testing using DocuSign's internally developed Sawmill tool.</i></p> <p><i>As part of DocuSign's SDLC process, QA captures evidence of test plan in Sawmill tool as the release packages move from testing, staging, and production environments. If there are security flaws identified during testing, QA, opens tickets in the developer's JIRA ticketing and includes the test results.</i></p> <p><i>In DocuSign Federal, DocuSign relies on the Arachni web application vulnerability scanners and the functionality of DocuSign Federal itself to identify any performance or security issues that are dynamically generated during the operation of the compiled codebase. Vulnerabilities and findings identified by the Arachni scanner is handled and remediated in accordance with RA-5. Performance monitoring issues or synthetic transaction failures identified by DocuSign Federal itself are handled at least monthly in accordance with the flaw remediation process described in SI-2.</i></p> <p><i>Any security flaws are documented and tracked within JIRA ticketing system to ensure developers mitigate the flaws prior to deployment within DocuSign Federal. The JIRA ticketing system captures the timeline of each</i></p>

SOLICITATION # ITS-400335

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				<i>security flaw to include the initial creation, milestones (e.g. approvals), and completion.</i>
6	Does the VENDOR implement automated mechanisms for incident handling and reporting? [IR-4 (1), IR-6 (1)]	X		<p>Our production systems are configured to send event and log data to a Security Information and Event Management (SIEM) system where events are correlated and analyzed by a dedicated team on a 24x7 basis.</p> <p>Responses to security events are initiated via alerts on our SIEM platforms. All devices in the DocuSign Enterprise network log to the SIEM. Alerts that are raised are typically actioned by our analysts in the 24x7 Security Operations Center, according to established Standard Operating Procedures. Events of a higher severity or complexity are handled by our Tier2/3 analysts in the CSIRT team. All incidents are documented in our Information Security Case Management (ISCM) system. Incident reporting functionality is within the ISCM system.</p> <p>We regularly research inconsistencies, conflicts, and non-logging devices as part of our operational procedures within the SOC, CSIRT, and Security Infrastructure teams. We even have specific advanced alerts that are tuned to recognize inconsistencies real-time, such as a user logging into two services in a span of time that is shorter than physically possible to travel.</p>
7	Does the VENDOR retain online audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and offline for at least one year to meet regulatory and organizational information retention requirements? [AU-7, AU-7 (1), AU-11]	X		At least 12 months
8	Does the VENDOR have the capability to notify customers and regulators of confirmed incidents in a timeframe consistent with all legal, regulatory, or contractual obligations? [State Incident Communications Procedures]	X		<p>State Incident Communications Procedures are a per contract agreement.</p> <p>DocuSign maintains a data breach notification program to promptly notify customers in the event their information is lost or experiences unauthorized access. DocuSign will promptly notify customers in</p>

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				<p>the event that their protected data is reasonably believed to be lost or stolen in an unencrypted format, or subject to unauthorized access by, or is used or disclosed as a result of an unauthorized acquisition. DocuSign will provide notice in writing promptly after discovery of such a security incident, but in no event later than the deadline set forth under applicable Law or the applicable business agreement, whichever is earlier.</p> <p>The written notice shall include, to the extent known, an identification of each individual whose personal information has been affected by the security incident, including state of residence; a brief description of the categories of personal information involved for each affected individual; a brief description of how and when the security incident occurred and how and when the security incident was discovered; and a brief description of any steps taken to address the security incident and any steps taken to prevent a recurrence.</p> <p>To the extent this information is not known when the initial written notice is first provided, DocuSign will promptly supplement the written notice, in writing when information becomes known (unless specifically directed otherwise by a law enforcement organization).</p>

Contingency Planning and Disaster Recovery

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Table 4-6. Contingency Planning and Disaster Recovery

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR have the capability to recover the system to a known and functional state following an outage, breach, DoS attack, or disaster? [CP-2, CP-2 (2), CP-2 (3), CP-9, CP-10]	X		<p>With DocuSign's Carrier Grade architecture, secure replication is performed in near real-time to our geo-diverse active systems.</p> <p>DocuSign designs all deployments to be fully redundant and fault tolerant.</p>

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				<p>There are no single points of failure in our load balanced, redundant configuration. Our environment uses load balancers to spread load throughout multiple servers. If a server fails or experiences an issue it should be transparent to users using our system. In addition to SQL clustering and server load-balancing we also have redundant networking gear that replicates customer documents up to 9 times across the systems that can recover in the event of a failure of any. All data is replicated at the OLTP level and all historical and document data is synchronized using a proprietary document replication service. The system is constructed to offer a worst case 5-minute recover point objective in the event of a single site catastrophic failure.</p> <p>Since data is replicated to geographically dispersed data centers traditional backups are unnecessary, while DocuSign does make 8 perpetual backups of blob data, along with weekly full and daily differential backups of the database as well as maintaining 5 active nodes. In the event of a disaster or total site failure in any of the active systems, all user activity is served by the remaining. DocuSign's failover capability is tested monthly during monthly site maintenance.</p> <p>Our DTM platform is closely monitored 24/7 for any malicious behavior including large, increased network throughput that may have the potential to impact our service.</p>

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				In the event of increased traffic, we can scale up to address inbound connections. We also have a Web Application Firewall (WAF) in place that allows us to block traffic based on various parameters.
2	Does the VENDOR have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with NIST Special Publication 800-34? [CP-2, CP-8]		X	<p>With DocuSign's Carrier Grade architecture, secure replication is performed in near real-time to our geo-diverse active systems. DocuSign designs all deployments to be fully redundant and fault tolerant. There are no single points of failure in our load balanced, redundant configuration. Our environment uses load balancers to spread load throughout multiple servers. If a server fails or experiences an issue it should be transparent to users using our system. In addition to SQL clustering and server load-balancing we also have redundant networking gear that replicates customer documents up to 9 times across the systems that can recover in the event of a failure of any. All data is replicated at the OLTP level and all historical and document data is synchronized using a proprietary document replication service. The system is constructed to offer a worst case 5-minute recover point objective in the event of a single site catastrophic failure.</p> <p>Since data is replicated to geographically dispersed data centers traditional backups are unnecessary, while DocuSign does make 8 perpetual backups of blob data, along with weekly full and daily differential backups of the database as well as maintaining 5 active nodes. In the event of a disaster or total site failure in any of the active systems, all user activity is served by the remaining. DocuSign's failover capability is tested monthly during monthly site maintenance.</p>

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
3	Does the system have alternate storage and processing facilities? [CP-6, CP-7]	X		<p>With DocuSign's Carrier Grade architecture, secure replication is performed in near real-time to our geo-diverse active systems. DocuSign designs all deployments to be fully redundant and fault tolerant. There are no single points of failure in our load</p>

				<p>balanced, redundant configuration. Our environment uses load balancers to spread load throughout multiple servers. If a server fails or experiences an issue it should be transparent to users using our system. In addition to SQL clustering and server load-balancing we also have redundant networking gear that replicates customer documents up to 9 times across the systems that can recover in the event of a failure of any. All data is replicated at the OLTP level and all historical and document data is synchronized using a proprietary document replication service. The system is constructed to offer a worst case 5-minute recover point objective in the event of a single site catastrophic failure.</p> <p>Since data is replicated to geographically dispersed data centers traditional backups are unnecessary, while DocuSign does make 8 perpetual backups of blob data, along with weekly full and daily differential backups of the database as well as maintaining 5 active nodes. In the event of a disaster or total site failure in any of the active systems, all user activity is served by the remaining. DocuSign's failover capability is tested monthly during monthly site maintenance.</p>
4	Does the system have or use alternate telecommunications providers? [CP-8, CP-8 (2)]	X		Our datacenters utilize redundant telecommunications providers
5	Does the system have backup power generation or other redundancy? [PE-11]	X		Yes, Backup Diesel Generators are utilized
6	Does the VENDOR have service level agreements (SLAs) in place with all telecommunications providers? [CP-8 (1)]	X		

Configuration and Risk Management

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Table 4-7. Configuration and Risk Management

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR maintain a current, complete, and accurate baseline configuration of the information system? [CM-2]	X		DocuSign Operations team maintains a Baseline Configuration Program.

SOLICITATION # ITS-400335

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				All corporate information and production systems are configured according to Baseline Configuration Standards to ensure capacity requirements. (We have proof of this with the server acceptance and deployment process and now also with Credentialed Scanning and CIS benchmarks.)
2	Does the VENDOR maintain a current, complete, and accurate inventory of the information system software, hardware, and network components? [CM-8]	X		DocuSign maintains a proprietary and confidential formal Asset Management Program which is ISO27001, PCI DSS, and SSAE16 examined and certified. DocuSign's production operations are housed within commercial-grade, secure datacenter facilities. Computer and communications equipment managed by DocuSign staff is physically isolated from equipment managed by third parties. All DocuSign computer and communications assets have a unique identifier attached to it such that physical inventories can be efficiently conducted as well as a sensitivity classification.
3	Does the VENDOR have a Configuration Management Plan? [CM-9, CM-11]	X		
4	Does the VENDOR follow a formal change control process that includes a security impact assessment? [CM-3, CM-4]	X		DocuSign maintains an ISO 27001, PCI DSS, and SSAE16 examined and tested Change Control policy and processes. All changes made to DocuSign Product Operations systems, Information, and devices are managed via the DocuSign tool. Changes are subjected to a testing regimen defined by IT and Technical Operations, which includes comprehensive scanning.

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				<p>Technology systems, network devices, security devices, Active Directory objects or logging mechanisms must be authorized prior to the change being made in accordance with a specifically defined and documented approval process.</p> <p>All changes are documented and approved via the DocuSign tool. DocuSign performs extensive pre-deployment testing as the preferred method for assurance of changes promoted into the production environment.</p>
5	Does the VENDOR employ automated mechanisms to detect inventory and configuration changes? [CM-2(2); CM-6(1), CM-8(3)]	X		<p>DocuSign manages the baseline operating system (OS) images of different components within the production environment to ensure OS configurations remain consistent and current in the Kickstart tool. The baseline OS images are configured and hardened in accordance with CM-6 and CM-7, and changes to the baseline OS images are carefully controlled using the change management processes described in CM-3 and CM-4.</p> <p>Additionally, DocuSign uses Windows Server Update Services and Yum-Update for Windows and CentOS hosts respectively, to ensure that all servers within the DocuSign Federal boundary are kept up-to-date with the most recent patches and security updates. Those updates are then added to the baseline images for the servers. DocuSign leverages DC Auto to store and deploy the updated baseline OS images.</p> <p>DocuSign relies on Amazon and Microsoft to maintain the baseline OS images for services operated in AWS and Azure respectively. Refer to the AWS and</p>

SOLICITATION # ITS-400335

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				Azure documentation packages for more information about the physical protections provided by these vendors.
6	Does the VENDOR prevent unauthorized changes to the system? [CM-5, CM-5(1), CM-5(5)]	X		Authorized Technical Operations members are reviewed, approved, and provisioned access to DocuSign Federal in accordance with AC-2, AC-3, and AC-5. System access is granted based on intended system usage, valid system access authorization and physical access, and responsibilities for mission/business functions. All Technical Operations members authorized to access DocuSign Federal are managed, identified, and authenticated in a consistent fashion in accordance with AC-2, IA-2, and IA-2(1).
<input type="checkbox"/>	<ul style="list-style-type: none"> Does the VENDOR establish configuration settings for products employed that reflect the most restrictive mode consistent with operational requirements? [CM-6] 	X		<i>Access Control and configuration is managed by the customer administrator</i>

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
8	Does the VENDOR ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP)-validated or SCAP-compatible (if validated checklists are not available)? [CM-6]		X	DocuSign actively scans all operating systems, infrastructure, databases, and web applications within DocuSign Federal at least monthly using both authenticated and unauthenticated scans. If new significant vulnerabilities are discovered in between monthly scans, DocuSign conducts on-demand scans on DocuSign Federal. Further, DocuSign engages with a 3PAO to scan the entire DocuSign Federal system boundary as part of the annual FedRAMP audit. DocuSign uses a combination of Tenable's Nessus Security Center to scan all operating systems and databases and Arachni to scan web application interfaces. Both scanners are centrally managed and updated automatically as part of normal operation before any new scan. The scanners provide a comprehensive overview of vulnerabilities that enumerate

SOLICITATION # ITS-400335

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				web application vulnerabilities; software flaws; as well as unnecessary ports, protocols, and services. Further, the Nessus scanner identifies any policy non-compliance and other improper configurations using SCAP-compliance checklists. Lastly, the tools produce scan results with quantifiable CVSS scores and a description of the process and plugin used to determine the vulnerability, as well as built-in vulnerability trend analysis, patch / flaw remediation suggestions, and the breadth and depth of the scan.

For the following questions, Vendors may use Table 4-18 “Continuous Monitoring Capabilities – Additional Details” to enter the capability descriptions, supporting evidence, and missing elements.

9	Does the VENDOR perform authenticated operating system/ infrastructure, web, and database vulnerability scans at least monthly, as applicable? [RA-5, RA-5(5)]	X		<p>DocuSign actively scans all operating systems, infrastructure, databases, and web applications within DocuSign Federal at least monthly using both authenticated and unauthenticated scans. If new significant vulnerabilities are discovered in between monthly scans, DocuSign conducts on-demand scans on DocuSign Federal. Further, DocuSign engages with a 3PAO to scan the entire DocuSign Federal system boundary as part of the annual FedRAMP audit.</p> <p>DocuSign uses a combination of Tenable’s Nessus Security Center to scan all operating systems and databases and Arachni to scan web application interfaces. Both scanners are centrally managed and updated automatically as part of normal operation before any new scan.</p> <p>The scanners provide a</p>
---	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------	---	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

			<p>comprehensive overview of vulnerabilities that enumerate web application vulnerabilities; software flaws; as well as unnecessary ports, protocols, and services. Further, the Nessus scanner identifies any policy non-compliance and other improper configurations using SCAP-compliance checklists. Lastly, the tools produce scan results with quantifiable CVSS scores and a description of the process and plugin used to determine the vulnerability, as well as built-in vulnerability trend analysis, patch / flaw remediation suggestions, and the breadth and depth of the scan.</p> <p>Information Security and Technical Operations analyze the scan results to determine whether the identified vulnerabilities are actionable; vulnerabilities are unfeasible to remediate due to operational constraints; or vulnerability are false positive/out-of-scope.</p> <p>When vulnerabilities are either unfeasible to remediate or false positive/out of scope, Compliance documents the rationale in accordance with CA-5. Actionable vulnerabilities are remediated in accordance with FedRAMP requirements: all high-risk vulnerabilities are remediated within 30 days; all moderate-risk vulnerabilities are remediated within 90 days; and all low-risk vulnerabilities are remediated within 180 days.</p> <p>All actionable vulnerabilities in DocuSign Federal are remediated in accordance with the process described below:</p>
--	--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<ul style="list-style-type: none">• For vulnerabilities that can be remediated using vendor-provided patches, DocuSign adheres to the following timelines for patch implementation: vendor patches deemed emergency security patches are implemented within seven (7) days of the release of the patch. Vendor patches deemed critical security patches are implemented within 30 days of the release of the patch. Non-security patches are implemented within 90 days of the release of the patch. Whenever possible, vendor-provided patches are tested in the DocuSign Federal staging environment prior to deployment to the DocuSign Federal production environment.<ul style="list-style-type: none">• For DocuSign Federal component misconfigurations or configurable vulnerabilities, DocuSign Operations Center and Technical Operations personnel work together as appropriate to ensure appropriate configurations are deployed or implemented for the vulnerable component within an appropriate timeline, depending on severity. Whenever possible, configuration changes are tested in the DocuSign Federal staging environment prior to implementation within the DocuSign Federal production environment.• For software or web application vulnerabilities that are dependent on coding changes, developers in Engineering work to ensure appropriate code changes are developed, tested, and deployed to remediate the identified vulnerability within the appropriate timeline, depending on the severity. Developers test code changes in the staging
--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

			<p>environment prior to deploying the release package in DocuSign Federal.</p> <p>All remediation efforts follow change management testing, approval, and deployment procedures described in CM-3. Information Security compares vulnerability scan results over time to determine any potential systemic trends or risks. A monthly report is generated from the scanners and disclosed to any relevant stakeholders, including Engineering, Technical Operations, Information Security, Compliance, and any Federal Agencies who require vulnerability scan results in order to perform continuous monitoring activities in accordance with CA-5, CA-7, and SI-2. Any systemic trends or risks are assigned a risk rating and then assigned to the appropriate team for remediation. Further, vulnerabilities are reported to DocuSign from CVE bulletins and other industry sources in accordance with SI-5.</p>
10	<p>Does the VENDOR demonstrate the capability to remediate High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days? [RA-5, <i>State Continuous Monitoring policy</i>]</p>	X	<p>DocuSign maintains a formal SDLC and related programs, such as Patch Management, which are ISO27001, PCI DSS, and SSAE16 examined and certified</p> <p>Patches are obtained from vendors and deployed on a monthly basis across all production environments and network vulnerability scans are conducted afterward. Emergency patches are immediately applied as needed and follow Change Management procedures. The following is the patch categories: Critical: Immediate High: 30 days</p>

			Medium; 90 days
11	When a High vulnerability is identified as part of ConMon activities, does the VENDOR consistently check audit logs for evidence of exploitation? [RA-5(8)]	X	<p>DocuSign actively scans all operating systems, infrastructure, databases, and web applications within DocuSign Federal at least monthly using both authenticated and unauthenticated scans. If new significant vulnerabilities are discovered in between monthly scans, DocuSign conducts on-demand scans on DocuSign Federal. Further, DocuSign engages with a 3PAO to scan the entire DocuSign Federal system boundary as part of the annual FedRAMP audit.</p> <p>DocuSign uses a combination of Tenable's Nessus Security Center to scan all operating systems and databases and Arachni to scan web application interfaces. Both scanners are centrally managed and updated automatically as part of normal operation before any new scan.</p> <p>The scanners provide a comprehensive overview of vulnerabilities that enumerate web application vulnerabilities; software flaws; as well as unnecessary ports, protocols, and services. Further, the Nessus scanner identifies any policy non-compliance and other improper configurations using SCAP-compliance checklists. Lastly, the tools produce scan results with quantifiable CVSS scores and a description of the process and plugin used to determine the vulnerability, as well as built-in vulnerability trend analysis, patch / flaw remediation suggestions, and the breadth and depth of the scan.</p> <p>Information Security and Technical Operations analyze the scan results to determine whether the identified vulnerabilities are actionable; vulnerabilities are unfeasible to remediate due to operational constraints; or vulnerability are false positive/out-of-scope.</p> <p>When vulnerabilities are either unfeasible to remediate or false positive/out of scope, Compliance documents the rationale in accordance with CA-5. Actionable</p>

			<p>vulnerabilities are remediated in accordance with FedRAMP requirements: all high-risk vulnerabilities are remediated within 30 days; all moderate-risk vulnerabilities are remediated within 90 days; and all low-risk vulnerabilities are remediated within 180 days.</p> <p>All actionable vulnerabilities in DocuSign Federal are remediated in accordance with the process described below:</p> <ul style="list-style-type: none"> • For vulnerabilities that can be remediated using vendor-provided patches, DocuSign adheres to the following timelines for patch implementation: vendor patches deemed emergency security patches are implemented within seven (7) days of the release of the patch. Vendor patches deemed critical security patches are implemented within 30 days of the release of the patch. Non-security patches are implemented within 90 days of the release of the patch. Whenever possible, vendor-provided patches are tested in the DocuSign Federal staging environment prior to deployment to the DocuSign Federal production environment. • For DocuSign Federal component misconfigurations or configurable vulnerabilities, DocuSign Operations Center and Technical Operations personnel work together as appropriate to ensure appropriate configurations are deployed or implemented for the vulnerable component within an appropriate timeline, depending on severity. Whenever possible, configuration changes are tested in the DocuSign Federal staging environment prior to implementation within the DocuSign Federal production environment. • For software or web application vulnerabilities that are dependent on coding changes, developers in Engineering work to ensure appropriate code changes are developed, tested, and deployed to remediate the identified vulnerability within the appropriate timeline, depending on the severity. Developers test code changes in the staging environment prior to deploying the release package in DocuSign Federal.
--	--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

				<p>All remediation efforts follow change management testing, approval, and deployment procedures described in CM-3. Information Security compares vulnerability scan results over time to determine any potential systemic trends or risks. A monthly report is generated from the scanners and disclosed to any relevant stakeholders, including Engineering, Technical Operations, Information Security, Compliance, and any Federal Agencies who require vulnerability scan results in order to perform continuous monitoring activities in accordance with CA-5, CA-7, and SI-2. Any systemic trends or risks are assigned a risk rating and then assigned to the appropriate team for remediation. Further, vulnerabilities are reported to DocuSign from CVE bulletins and other industry sources in accordance with SI-5.</p>
--	--	--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Data Center Security

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Table 4-8. Data Center Security

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR restrict physical system access to only authorized personnel? [PE-2 through PE-6, PE-8]	X		<p>DocuSign is ISO 27001 certified and maintains formal policies and procedures including our DocuSign Access Control policy.</p> <p>DocuSign's employee logical access authorization chain requires direct manager approval, application/data source owner approval and, in cases of sensitive applications and data sources, security management approval. Access to critical applications and data sources is removed at employee termination and is reviewed at least quarterly to verify that appropriate and current access levels are maintained.</p> <p>DocuSign enforces the rule of least privilege and has documented segregation of duties. DocuSign enforces formal logical and account separation of the development, QA, and production environments.</p>
2	Does the VENDOR monitor and log physical access to the information system, and maintain access records? [PE-6, PE-8]	X		<p>Cyxtera, SunGard, and Equinix maintain physical access logs for the data center facilities for at least one year. Also, the</p>

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				<p>DocuSign cages in the Cyxtera, SunGard, and Equinix datacenter facilities are secured with industry-standard physical access control devices that are managed and monitored by DocuSign's Physical Security members.</p> <p>DocuSign relies on AWS, Azure, and Akamai to maintain physical access log for their data centers. No DocuSign personnel have access to their data centers. Refer to the AWS, Azure, and Akamai documentation packages for more information about physical access by these vendors.</p> <p>Cyxtera, SunGard, and Equinix review physical access logs at least quarterly or in the event of an identified security incident. Technical Operations also conducts a quarterly access review by requesting physical access logs from Cyxtera, SunGard, and Equinix and reviewing DocuSign's logical access logs.</p> <p>DocuSign relies on AWS, Azure, and Akamai to review physical access log for their data centers and notify DocuSign of any security incidents. No DocuSign personnel have access to their data centers. Refer to the AWS, Azure, and Akamai documentation packages for more information about physical access by these vendors.</p> <p>Technical Operations coordinate the results of the quarterly access reviews and incident investigations per the incident response policy.</p> <p>DocuSign relies on AWS, Azure, and Akamai to coordinate reviews and incidents for their data centers and notify DocuSign of any security incidents. No DocuSign personnel have access to their data centers. Refer to the AWS, Azure, and Akamai documentation packages for more information about physical access by these vendors.</p>
3	Does the VENDOR monitor and respond to physical intrusion alarms and surveillance equipment? [PE-6 (1)]	X		

Policies, Procedures, and Training

The Vendor must indicate the status of policy and procedure coverage for the NIST 800-53 Rev 4-families listed in Table 4- 9 below.

To answer "yes" to a policy, it must be fully developed, documented, and disseminated; and it must address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. A single policy document may address more than one family provided the NIST requirements of each "-1" are fully addressed.

To answer "yes" to a procedure, it must be fully developed and consistently followed by the appropriate staff. List all applicable procedure documents for each family.

VENDORS must establish their own set of Policies and Procedures (P&Ps). They cannot be inherited from a leveraged system, nor can they be provided by the customer. Any exceptions and/or missing policy and procedure elements must be explained in Table 4-10 below.

Table 4-9. Policies and Procedures

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
1	Access Control [AC-1]		X		X	Standard: 240.1.2-5.02 – August 2017
2	Awareness & Training [AT-1]		X		X	Standard: 220.2.1.015 – August 2017
3	Audit & Accountability [AU-1]	X			X	Policy: <input type="checkbox"/> 240.1.03-03.00 – December 2017
4	Security Assessment & Authorization [CA-1]	X				Policy: <input type="checkbox"/> 253.1.01.212 August 2017
5	Configuration Management [CM-1]		X		X	Standard: 130.2.03.014 - July 2017
6	Contingency Planning [CP-1]		X	X		Policy: <input type="checkbox"/> 130.2.03.014 February 2018

SOLICITATION # ITS-400335

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
7oi	Identification & Authentication [IA-1]	X			X	Policy: <input type="checkbox"/> 130.2.03.014 February 2018
8	Incident Response [IR-1]		X		X	Standard: 240.2.01.208 – July 2017
9	Maintenance [MA-1]	X			X	Policy: <input type="checkbox"/> 250.1.008.01.09 August 2016
10	Media Protection [MP- 1]	X			X	Policy: <input type="checkbox"/> 253.1.01.212 August 2017
11	Physical & Environmental Protection [PE-1]	X			X	Policy: 240.1.01.118 – August 2017
12	Personnel Security [PS- 1]	X			X	Policy: 220.1.01.014 – August 2017
13	Risk Assessment [RA-1]		X	X		Policy: 240.2.02.206 – July 2017
14	System & Services Acquisition [SA-1]	X			X	Policy: 130.2.03.009 – July 2017
15	System & Communications Protection [SC-1]	X			X	Policy: 253.1.01.212 – August 2017
16	System & Information Integrity [SI-1]	X			X	Policy: 310.3.01.017 – September 2017

SOLICITATION # ITS-400335

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
17	Planning [PL-1]	X			X	Policy: 253.1.01.212 – August 2017

For any family with a policy or procedure gap, please describe the gap below.

Table 4-10. Missing Policy and Procedure Elements

Missing Policy and Procedure Elements
•

The Vendor must answer the questions below.

Table 4-11. Security Awareness Training

Question	Yes	No	Describe capability, supporting evidence, and any missing elements
Does the VENDOR train personnel on security awareness and role-based security responsibilities?	X		<p>DocuSign team members complete Security Awareness Training upon hiring and annually thereafter. Acknowledgement of training is tracked via the SAP Success Factors Learning Management System (LMS). In addition, ongoing security awareness activities occur throughout the year so that security stays top of mind with DocuSign team members. This includes quarterly security newsletters, Chatter group posts in salesforce.com, and Lunch & Learn sessions.</p> <p>Annual and New Hire Security Awareness training topics include:</p> <ul style="list-style-type: none"> • Security policies • Use of company assets • Acceptable use • Personal data and privacy • Spam and malware • Passwords • Access control • Visitors and badging • Clean desk and workspace • Mobile device protection • Incident response • Business continuity/disaster recovery • Manager responsibilities • Information classification guidelines • Protecting sensitive data • Information Policy Acknowledgement <p>Upon completion of the course, DocuSign team members are required to complete a test to gauge learning effectiveness and must pass with a minimum score of 90%. Successful completion of the test is recorded in the LMS.</p>

SOLICITATION # ITS-400335

Question	Yes	No	Describe capability, supporting evidence, and any missing elements
			In addition to taking this course, new hires are also provided overviews of security responsibilities on their first day in the office as well as in Discovering DocuSign, a two-day overview of DocuSign.

Additional Capability Information

State will evaluate the responses in this section on a case-by-case basis relative to a State-Ready designation decision.

Staffing Levels

In the table below, the Vendor must describe the VENDOR's organizational structure, staffing levels currently dedicated to the security of the system, as well as any planned changes to these staffing levels. This description must clearly indicate role and number of individuals as well as identify which staff is full-time dedicated, and which are performing their role as a collateral duty.

Table 4-12. Staffing Levels

Staffing Levels DocuSign Staffing, Organization and Number of Employees by function is Restricted

Change Management Maturity

While the following change management capabilities are not required, they indicate a more mature change management capability and may influence a State Readiness decision, especially for larger systems.

The Vendor must answer the questions below.

Table 4-13. Change Management

#	Question	Yes	No	If "no", please describe how this is accomplished.
1	Does the VENDOR's change management capability include a fully functioning Change Control Board (CCB)?	X		<p>DocuSign maintains an ISO 27001, PCI DSS, and SSAE16 examined and tested Change Control policy and processes. All changes made to DocuSign Product Operations systems, Information, and devices are managed via the DocuSign tool. Changes are subjected to a testing regimen defined by IT and Technical Operations, which includes comprehensive scanning.</p> <p>Technology systems, network devices, security devices, Active Directory objects or logging mechanisms must be authorized prior to the change being made in accordance with a specifically defined and documented approval process.</p> <p>All changes are documented and approved via the DocuSign tool.</p> <p>DocuSign performs extensive pre-deployment testing as the preferred method for assurance of changes promoted into the production environment.</p>
2	Does the VENDOR have and use development and/or test environments to verify changes before implementing them in the production environment?	X		<p>DocuSign utilizes industry standards to build-in security for our Systems/Software Development Lifecycle (SDLC). DocuSign implements a</p>

SOLICITATION # ITS-400335

#	Question	Yes	No	If "no", please describe how this is accomplished.
				<p>formal SDLC that is fully documented and audited as part of its SSAE 16 audit and ISO 270001 certifications. The formal SDLC is based on Scrum Agile.</p> <p>Code is developed in individual development environments through developer unit test and then deployed to a formal QA environment for testing, verification and requirements review by the separate QA and product management teams.</p> <p>DocuSign does not use customer data in development or testing.</p> <p>DocuSign's application security follows industry best practices (OWASP) Annual 3rd party external PEN tests are conducted along with a minimum of quarterly internal application vulnerability scanning.</p> <p>DocuSign has a formal software development lifecycle that includes secure coding practices against OWASP and related standards. DocuSign's process is continually validated through internal evaluation and testing, and with qualified-3rd party validation. DocuSign's production environment is a dedicated, secure facility that undergoes the same rigor of testing as our application.</p> <p>DocuSign's approach aligns with international standards to continually improve through ongoing assessment and implementation practice.</p>

SOLICITATION # ITS-400335

#	Question	Yes	No	If "no", please describe how this is accomplished.
				consistent with the cycle of plan, do, check act (PDCA).

Vendor Dependencies and Agreements

The Vendor must answer the questions below.

Table 4-14. Vendor Dependencies and Agreements

#	Question	Yes	No	Instructions
1	Does the system have any dependencies on other vendors such as a leveraged service offering, hypervisor and operating system patches, physical security and/or software and hardware support?	X		
2	Within the system, are all products still actively supported by their respective vendors?	X		If any are not supported, answer, "No."
3	Does the VENDOR have a formal agreement with a vendor, such as for maintenance of a leveraged service offering?	X		If "yes," please complete Table 4-16. Formal Agreements Details below.

If there are vendor dependencies, please list each in the table below, using one row per dependency. For example, if using another vendor's operating system, list the operating system, version, and vendor name in the first column, briefly

indicate the VENDOR's reliance on that vendor for patches, and indicate whether the vendor still develops and issues

patches for that product. If there are no vendor dependencies, please type "None" in the first row.

Table 4-15. Vendor Dependency Details

#	Product and Vendor Name	Nature of Dependency	Still Supported?	
			Yes	No
1	Microsoft Windows Server	Product Environment	X	
2	CentOS	Product Environment	X	
3	Cyxtera	Datacenter Hosting	X	
4	SunGard	Datacenter Hosting	X	
5	F5	Product Networking	X	

If there are formal vendor agreements in place, please list each in the table below, using one row per agreement. If there

are no formal agreements, please type "None" in the first row.

Table 4-16. Formal Agreements Details

#	Organization Name	Nature of Agreement
1		
2		

SOLICITATION # ITS-400335

DocuSign has a formal Legal, Contracts, and Regulatory Program that is ISO 27001 certified and ensures compliance with applicable laws. Legal counsel reviews all third party agreements and Security has a formal Third Party Security Assessment. DocuSign subcontractors are professional, commercial grade datacenters and Tier 1 customer service included within ISO 27001 certification.

DocuSign leases datacenter space (ping, pipe, power) from various facilities. Datacenters are PCI DSS compliant and SSAE examined by their own auditors.

DocuSign owns the hardware, software (or software licenses where applicable) and applications (application licenses where applicable) within the leased datacenter space.

DocuSign hosts the application on DocuSign owned equipment within the leased datacenter space.

Continuous Monitoring Capabilities

In the tables below, please describe the current state of the VENDOR's Continuous Monitoring capabilities, as well as the

length of time the VENDOR has been performing Continuous Monitoring for this system.

Table 4-17. Continuous Monitoring Capabilities

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR have a lifecycle management plan that ensures products are updated before they reach the end of their vendor support period?	X		DocuSign utilizes industry standards to build-in security for our Systems/Software Development Lifecycle (SDLC) DocuSign implements a formal SDLC that is fully documented and audited as part of its SSAE 16 audit and ISO 270001 certifications. The formal SDLC is based on Scrum Agile. Code is developed in individual development environments through developer unit test and then deployed to a formal QA environment for testing.

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				<p>verification and requirements review by the separate QA and product management teams. DocuSign does not use customer data in development or testing. DocuSign's application security follows industry best practices (OWASP) Annual 3rd party external PEN tests are conducted along with a minimum of quarterly internal application vulnerability scanning. DocuSign has a formal software development lifecycle that includes secure coding practices against OWASP and related standards. DocuSign's process is continually validated through internal evaluation and testing, and with qualified-3rd party validation. DocuSign's production environment is a dedicated, secure facility that undergoes the same rigor of testing as our application. DocuSign's approach aligns with international standards to continually improve through ongoing assessment and implementation practice consistent with the cycle of plan, do, check act (PDCA).</p>
2	Does the VENDOR have the ability to scan all hosts in the inventory?	X		Our production systems are configured to send event and

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
				<p>log data to a Security Information and Event Management (SIEM) system where events are correlated and analyzed by a dedicated team on a 24x7 basis.</p> <p>Responses to security events are initiated via alerts on our SIEM platforms. All devices in the DocuSign Enterprise network log to the SIEM. Alerts that are raised are typically actioned by our analysts in the 24x7 Security Operations Center, according to established Standard Operating Procedures. Events of a higher severity or complexity are handled by our Tier2/3 analysts in the CSIRT team. All incidents are documented in our Information Security Case Management (ISCM) system. Incident reporting functionality is within the ISCM system.</p> <p>We regularly research inconsistencies, conflicts, and non-logging devices as part of our operational procedures within the SOC, CSIRT, and Security Infrastructure teams. We even have specific advanced alerts that are tuned to recognize inconsistencies real-time, such as a user logging into to two services in a span of time that is shorter than physically possible to travel.</p>
3	Does the VENDOR have the ability to provide scan files in a structure data format, such as CSV, XML, or .nessus files?		X	<p>Scan Files are DocuSign Restricted.</p> <p>Please see annotated scans within the DocuSign Security and Trust Assurance Packet for details</p>
4	Is the VENDOR properly maintaining their Plan of Actions and Milestones (POA&M), including timely, accurate, and complete information entries for new scan findings, vendor check-ins, and closure of POA&M items?	X		<p>Please see DocuSign Security and Trust Assurance Packet for details</p>

In the table below, provide any additional details the Vendor believes to be relevant to State's understanding of the VENDOR's Continuous Monitoring Capabilities. If the Vendor has no additional details, please state, "None."

Table 4-18. Continuous Monitoring Capabilities – Additional Details

Continuous Monitoring Capabilities – Additional Details

DocuSign has implemented a continuous monitoring strategy that encompasses vulnerability scanning and management processes in accordance with

- RA-5 and SI-2 requirements
- Annual security assessments in accordance with CA-2
- POA&M management processes in accordance with CA-5
- Periodic security reauthorization in accordance with CA-6
- Annual penetration testing in accordance with CA-8
- Continuous network monitoring in accordance with SI-4

In addition to these explicit requirements, DocuSign also reviews and updates all security documentation associated with the information system at least annually to ensure accuracy and currency. DocuSign has implemented this strategy in accordance with FedRAMP-required timelines.

Status of System Security Plan (SSP)

In the table below, explicitly state whether the SSP is fully developed, partially developed, or non-existent. Identify any sections that the VENDOR has not yet developed.

Table 4-19. Maturity of the System Security Plan

Maturity of the System Security Plan

SSP is fully developed

In the table below, state the number of controls identified as "Not applicable" in the SSP. List the Control Identifier for each, and indicate whether a justification for each has been provided in the SSP control statement.

Table 4-20. Controls Designated "Not Applicable"

<> Controls are Designated "Not Applicable"

In the table below, state the number of controls with an alternative implementation. List the Control Identifier for each.

Table 4-21. Controls with an Alternative Implementation

<x> Controls have an Alternative Implementation

Addendum 1 Confirmation

Please find the Addendum 1 confirmation on the following page.



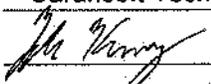
Solicitation Addendum

Solicitation Number: ITS-400335
Solicitation Description: Enterprise Electronic Forms and Digital Signature Capability
Solicitation Opening Date and Time: July 12, 2018 @ 2:00pm
Addendum Number: 1
Addendum Date: June 11, 2018
Contract Specialist or Purchasing Agent: Kristen Burnette, Contract and Vendor Manager
Kristen.burnette@nc.gov 919-754-6678

-
1. This addendum does not need to be returned.
 2. Special instructions on Interactive Purchasing System (IPS) was corrected to show the following:

Enterprise Electronic Forms and Digital Signature Capability RFP
Written questions must be submitted by 2:00pm on June 21, 2018.

Execute Addendum:

Offeror: Carahsoft Technology Corporation
Authorized Signature: 
Name and Titled (Typed): Zak Kennedy, Account Representative
Date: 7/23/18

Addendum 2 Confirmation

Please find the Addendum 2 confirmation on the following page.

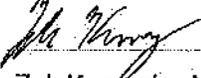


Solicitation Addendum

Solicitation Number: ITS-400335
Solicitation Description: Enterprise Electronic Forms and Digital Signature Capability
Solicitation Opening Date and Time: July 24, 2018 @ 2:00pm
Addendum Number: 2
Addendum Date: July 9, 2018
Contract Specialist or Purchasing Agent: Kristen Burnette, Contract and Vendor Manager
Kristen.burnette@nc.gov 919-754-6678

-
1. This addendum does not need to be returned.
 2. The solicitation is hereby modified as follows:
 - M1. The RFP ITS-400335 Bid opening has been extended to: **July 24 at 2:00 PM EST.**

Execute Addendum:

Offeror: Carahsoft Technology Corporation
Authorized Signature: 
Name and Titled (Typed): Zak Kennedy, Account Representative
Date: 7/23/18

Addendum 3 Confirmation

Please find the Addendum 3 confirmation beginning on the following page:



Solicitation Addendum

Solicitation Number: ITS-400335
Solicitation Description: Enterprise Electronic Forms and Digital Signature Capability
Solicitation Opening Date and Time: July 24, 2018 @ 2:00pm
Addendum Number: 3
Addendum Date: July 11, 2018
Contract Specialist or Purchasing Agent: Kristen Burnette, Contract and Vendor Manager
Kristen.burnette@nc.gov 919-754-6678

1. Return one properly executed copy of this addendum with bid response prior to the Solicitation Opening Date and Time listed above.
2. **This solicitation is hereby modified to remove Section II, 6) Branding.**
3. Following are questions received about the solicitation and the State's answers to the questions.

Question #	Vendor Question	The State's Response
1	Please confirm that you will you consider two different solutions, one for enterprise electronic forms and one for digital signatures. Can we respond to the one solution we offer and disregard the items for the one we do not?	We are looking for a turnkey solution like we have today which allows for forms and Signature.
2	What electronic signature vendor are you replacing? Why? Cost? Functionality?	The purpose of this RFP is to establish a multi-vendor/ multi-solution statewide convenience contract. Our current solution is DocuSign which could be included on the new Statewide contract.
3	Will the state be open to accepting (Since SaaS offerings are multi-tenant) the T&C's of the vendor? Unless it is run in a private cloud, a public cloud must serve multi-tenants and particular T&C's are applicable to all.	The State will review all vendor-submitted terms and conditions and accept those that best meet the state's needs. We need to understand the architecture and separation of customers from a security perspective. Data must also remain in the Continental US.
4	Have you evaluated and/or been presented with demos/meetings from other e-signature vendors already year to date?	No

Question #	Vendor Question	The State's Response
5	Will you be open to a conversation/demo between key stakeholders and vendor - prior to the submission of a response to make sure that the vendor and state are on the same page as to need, functionality etc.?	Conversations/ demos will not be done prior to the bid submissions.
6	You mention that up to 65K transactions will be procured. Is that for the 1 st year or over a number of years? What do you see as the minimum amount of transactions purchased in the first year?	65,000 transactions are the current annual usage. We used historical figures in the RFP. We are unable to give the minimum amount of transactions the first year.
7	Will there be any need for on premise solution?	No, the State is seeking a SaaS solution We are not wanting to build an on-premise solution. This is a decentralized solution and need the Vendor to take care of operations, configurations and administration.
8	As the State intends to provide more than one Cloud Based Software solution, does the State currently offer solutions hosted in Azure? Are their contracts in place with Microsoft in this regard that can be leveraged?	The state is looking for a SaaS Solution offered by the vendor. The Vendor should use their own Cloud/Infrastructure and not the State's.
9	As the table only indicates up to 25 named user, can you confirm there are no more than 25 named users who will create forms templates and capture data on these forms for processing? Are the transactional numbers listed for public facing forms only or are these transaction numbers in lieu of named users?	<p>At some point there will be a break even or business reason to move to transaction based pricing. Vendor must provide pricing up to 25 named users. Vendor can provide pricing for more than 25 if they want to.</p> <p>Vendor is encouraged to recommend when one solution makes more sense than the other.</p> <p>The vendor should identify costs for public facing form sign offs.</p>
10	Is the list provided definitive? Are we to assume therefore that licenses for commodity databases such as SQL Server are not available via the state and thus must be licensed for this project separately?	We want a turnkey SaaS solution. Vendor's licensing should include all costs for providing that solution.
11	The cited Branding guide is protected by an ID / password challenge. Can the state please provide this to bidders?	Removed in #2 above.

Question #	Vendor Question	The State's Response
12	Can the state elaborate over what timespan the 95,000 transactions are expected? Is this annual expected usage? Does this include both internal named users as well as a Customer Facing Web Portal to Serve the public (non-employees) of the State?	This RFP initiative calls for an Indefinite Quantity Contract but typically, this is the estimated yearly amount. Yes, it will include both internal and external users.
13	Will the solution need to integrate with 3rd party signature software such as DocuSign?	No.
14	Will the solution need to integrate with a Content Management System such as Drupal or WordPress?	The solution will need to potentially integrate with content management systems. We have asked for connectors or the ability to integrate to Dynamics 365, Salesforce, SharePoint Online and on Prem. Solution provides Application Programming Interfaces (APIs) for integration with other Customer systems. Include any details on Application Programming Interfaces (APIs) provided.
15	How often would data need to be transferred to internally hosted systems? Hourly? Daily?	Hourly at a minimum, and if possible, in real-time.
16	Do you require form analytics and/or data visualization?	The State considers these "nice to have," but not required.
17	Will the solution need to have multilingual capabilities for forms in different languages?	Yes.
18	Any specific requirements for level of web content accessibility i.e. WCAG 2.0 A - AAA?	Yes, State requires the build be WCAG 2.0 AA compliant.
19	What is the preferred format for references?	Format of references is at the discretion of the vendor; however at a minimum, vendors are expected to include name, phone number/email, and title and company of the individual providing the reference.
20	Is there a specific Cloud Service Provider the State prefers for this RFP i.e. AWS, Azure, other...	The state is looking for a SaaS Solution offered by the vendor. The Vendor should use their own Cloud/Infrastructure and not the State's.
21	Does the State currently have usage analytics such as monthly traffic, average downloads, etc.?	The State currently uses Tableau and PowerBi. The State does require a rolled-up view of utilization both quarterly and yearly.
22	Have all of the existing forms already been converted to PDF format?	No.
23	Does each agency have an index or catalog of their forms?	No.
24	Does the current infrastructure facilitate network communication with all agencies using forms?	No.

Question #	Vendor Question	The State's Response
25	Do all forms reside on the same domain?	No.
26	Is there a predominant platform in use and if so what is it? (Windows, Unix, Ubuntu, etc.)	Windows Office 365.
27	Do all network subscribers currently have digital signatures	No.
28	Are all ad hoc work flows identified and documented throughout the enterprise?	No.
29	Does current Enterprise use Active Directory or some other directory service? If so, which one?	Most agencies use the State's Enterprise Active Directory Service (EADS) via SAML, but not all. However, all Agencies use NCID for Authentication.
30	Is there currently a predominant internet browser throughout the Enterprise or will vendor provide support for all browser types?	There is no predominant internet browser. Browsers should be N-1 and vendors should describe if the solution facilitates digital signing of documents via a computer web browser with modern browsers. Specify minimum software versions supported.
31	Is it an assumption that in the 12 months, all of the 95,000 transactions will have digital signature capability?	95,000 transactions is an annual estimate, but this will be an indefinite quantity contract. Number of transactions is not guaranteed.
32	Does NCID manage Enterprise Digital Signatures? If so, who is the point of contact?	No.
33	Does NCID manage all security groups?	NCID only does authentication, not application authorization.
34	Which directory service AD or is used?	The State's active directory (AD) service uses Microsoft Active Directory.
35	For pre-population, does the State have forms that already auto populate? If not, do all forms that need the pre-populate feature have business processes associated with them?	Some agencies may have forms that prepopulate, but this functionality is not available across the state.
36	Does the State know the location of the site where the current repositories for forms are stored? How many years has the current repository existed? What is the current size of it?	Each agency has a respective repository. Age and size are unknown.
37	Does the State know by location, region or area, the current number of reports being used in each area? If so, what is the approximate breakdown by location, region or area?	The State does not have this information.

Question #	Vendor Question	The State's Response
38	Will the State use their own existing service desk or will the vendor be required to establish service operations for Enterprise Forms Solutions?	The Vendor to provide support for the solution.
39	Will an online LMS style be a viable option for an Enterprise Solution?	Yes, Vendors are encouraged to provide multiple training options.
40	Will training be provided throughout the forms life cycle?	Yes, ideally training will include an array of users up to Administrator.
41	Is training the responsibility of the vendor or will the State facilitate their own training?	The State prefers the Vendor to assume training responsibility; the State is open to "train-the-trainer" or "on-demand training for all levels" types of environments.
42	What type of integration is the State looking for with NCID? Is this a method to authenticate citizens, or is this for internal users?	Users with an NCID should be able to authenticate. Non NCID users should be able to be involved in work flow and business process. The Vendor is encouraged to elaborate on what authentication methods can be provided for non NCID users.
43	Can the State elaborate on the intended use case for capturing a picture of the signature owner with the signature?	The ideal solution will capture a picture of the owner's signature and associate it with the actual signature.
44	Does the State have any restrictions around the graphical image of the signature? If so, what are they?	No.
45	Can the State elaborate on what is intended by capture speed and pressure? Is there a specific use case where this would be a requirement?	No.
46	Can the state provide additional information on the requirements for redlining?	Redlining will allow users in a workflow to make changes and have those changes be routed to the originator and all previous signers.
47	Do you require proven performance/experience in the state of North Carolina with state and local agencies? If not required, is it preferred?	No, per the RFP, preferred evaluation criteria consists of the Vendor's corporate background and similar experience, specifically the technical situations, specifications, needs, challenges, and opportunities.
48	Is there a small business preference?	No; however, pursuant to N.C.G.S. §§143B-1361(a), 143-48 and 143-128.4 and any applicable Executive Order, the State invites and encourages participation in this procurement process by businesses owned by minorities, women, disabled, and disabled business enterprises.

Question #	Vendor Question	The State's Response
49	Is the state using the term "Digital Signature" and "Electronic Signature" interchangeably? All Digital signatures are electronic signatures, but not all electronic signatures are digital signatures.	Yes, we are used interchangeably.
50	Does the State prefer a vendor who has FedRAMP authorized Moderate who can handle PHI/PII for state agencies? Vendors that are FedRAMP authorized Low are not certified by FedRAMP to handle PHI/PII.	Data stored in the e-Forms/e-Signature Program may be classified from public up to Highly Restricted. Therefore, the e-Forms/e-Signature Program should be classified as NIST Moderate per the Statewide Information Security Manual and must be capable of receiving and securely managing data that is classified up to Restricted or Highly Restricted per the State's Data Classification and Handling Policy. To comply with policy, assessment reports such as the Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, and ISO 27001 are preferred and offered solutions already meeting these requirements are requested to include these reports as part of their submission.
51	Do you have required minimums for uptime?	No.
52	Regarding uptime statistics, would the State prefer for vendors to provide the following metrics?	Yes.
53	-Historical uptime for the last 3 months, 6 months, and 12 months	Yes.
54	-Uptime inclusive of maintenance windows	Yes.
55	-Average hours the system is scheduled to be down for maintenance	Yes.
56	Does the State prefer to have uptime reporting to be inclusive of maintenance windows?	Yes.
57	Does the State prefer a vendor to report	Yes.
58	If the state does mean, digital signatures, who will be the certificate authority? Is the state planning on being the certificate authority?	The solution can be electronic signature or digital signature. The state will not be the digital certificate authority. The solution shall produce an esigned pdf which is automatically trusted and validated by Adobe when opened by Adobe.

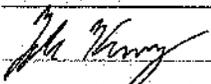
Question #	Vendor Question	The State's Response
59	Is the state looking for providers that provide the digital/e-signature, e-forms, and workflow capabilities under one brand?	Yes.
60	Can a vendor that supplies an e-form and workflow solution that integrates with solutions like Adobe Sign and DocuSign, submit a response for these sections of the RFP only.	We are looking for a turnkey solution like we have today which allows for forms and Signature.
61	Section III - Page 25 10d - Are NCDIT referring to the digital certificate that is wrapped around an electronically signed document?	The solution needs to generate an electronically or digitally signed PDF that is automatically verified as a valid e-signed PDF when opened by Adobe Reader.
62	Section III - 3.6 – The link to branding guidelines is password protected. Can you please provide us access to the branding guidelines referenced in the RFP document?	Removed in #2 above.
63	Does NCDIT require custom domains in their URLs?	All URLs must be https.
64	Section III - 3.11 – RFP States: <i>“Based on current usage, the State estimates that the solution will eventually accommodate over 95,000 transactions”</i> , Question: Over what timeframe?	Yearly.
65	Does the cost for back end integrations need to be included? If so, which integrations specifically need to have a price called out? If there are any integrations (non-implementation) for pre-built product integrations?	All costs should be specified for making the integration with NCID and various Connectors.
66	Do costs for annual support costs need to be called out in the response? If so, how detailed do we need to provide.	All Potential Costs should be supplied.
67	Do you need to know if there are any costs for onboarding or account management? Per hour or one-time charges?	All Potential Costs should be supplied.
68	If this is a state-wide implementation, will 96,000 transactions cover all interested agencies and is this an annual figure or aggregate for the term of the contract?	This number is an annual figure.

4. Failure to acknowledge receipt of this addendum may result in rejection of the response.

Check ONE of the following options:

- Bid has not been mailed. Any changes resulting from this addendum are included in our bid response.
- Bid has been mailed. No changes resulted from this addendum.
- Bid has been mailed. Changes resulting from this addendum are as follows:

Execute Addendum:

Vendor/ Offeror: Carahsoft Technology Corporation
Authorized Signature: 
Name and Titled (Typed): Zak Kennedy, Account Representative
Date: 7/23/18

