ENTERPRISE SECURITY & RISK MANAGEMENT OFFICE (ESRMO)



Vendor Readiness Assessment Report (VRAR)

for Solutions Hosted on State Infrastructure

# Executive Summary

The State requires all systems that are connected to the State network or that process State data meet an acceptable level of security compliance. The State of NC has adopted the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 as the foundation for identifying and implementing information technology security controls. These controls are described in the Statewide Information Security Manual (SISM).

The following is a high-level view of specific security requirements for a solution that is hosted on the State network to meet compliance. The control references (e.g. AC-2) refer to the specific NIST 800-53 control as listed in the SISM, which may be found at the following link: <https://it.nc.gov/statewide-information-security-policies>.

**Note**: There may be additional requirements depending on the sensitivity of the data, other Federal and State mandates, or agency specific requirements.

Table of Contents

[Executive Summary i](#_Toc525047584)

[1. Introduction 1](#_Toc525047585)

[1.1. Purpose 1](#_Toc525047586)

[1.2. Outcomes 1](#_Toc525047587)

[1.3. State Approach and Use of This Document 1](#_Toc525047588)

[2. VENDOR System Information 2](#_Toc525047589)

[2.1. Data Flow Diagrams 2](#_Toc525047590)

[2.2. Separation Measures [AC-4, SC-2, SC-7] 2](#_Toc525047591)

[3. Capability Readiness 3](#_Toc525047592)

[3.1. State Mandates 3](#_Toc525047593)

[3.2. State Requirements 3](#_Toc525047594)

[3.2.1. Approved Cryptographic Modules [SC-13] 3](#_Toc525047595)

[3.2.2. Transport Layer Security [NIST SP 800-52, Revision 1] 4](#_Toc525047596)

[3.2.3. Identification and Authentication, Authorization, and Access Control 4](#_Toc525047597)

[3.2.4. Audit, Alerting, Malware, and Incident Response 5](#_Toc525047598)

[3.2.5. Configuration and Risk Management 5](#_Toc525047599)

[3.3. Additional Capability Information 6](#_Toc525047600)

[3.3.1. Change Management Maturity 6](#_Toc525047601)

[3.3.2. System and Services Acquisition 6](#_Toc525047602)

List of Tables

[Table 2-1. System Information 2](#_Toc524443554)

[Table 3-1. State Mandates 3](#_Toc524443555)

[Table 3-2. Cryptographic Modules 3](#_Toc524443556)

[Table 3-3. Transport Layer Security 4](#_Toc524443557)

[Table 3-4. Identification and Authentication, Authorization, and Access Control 4](#_Toc524443558)

[Table 3-5. Audit, Alerting, Malware, and Incident Response 5](#_Toc524443559)

[Table 3-6. Configuration and Risk Management 5](#_Toc524443560)

[Table 3-7. Change Management 6](#_Toc524443561)

# Introduction

## Purpose

This report and its underlying assessment are intended to enable State agencies to reach a state-ready decision for a specific solution that will be hosted on the State network based on organizational processes and the security capabilities of the Moderate/low-impact information system.

## 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 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 the State to render a readiness decision based on a more complete understanding of the vendor’s security capabilities.

Section 3, Capability Readiness, is organized into three sections:

* **Section 3.1, State Mandates**, identifies a small set of the state mandates a vendor must satisfy. The State **will not** waive any of these requirements.
* **Section 3.2, 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 3.3, 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. The VRAR template is intended for systems categorized at the Moderate security impact level, in accordance with the FIPS Publication 199 Security Categorization.

Table 2-1. System Information

|  |
| --- |
| VENDOR Name:Solution/System Name:FIPS PUB 199 System Security Level: (Moderate)Number of Customers (State/Others): Enter # of customers / # of other customersSystem Functionality: Briefly describe the functionality of the system and service being provided.  |

## Data Flow Diagrams

Insert Vendor-validated data flow diagram(s), and provide a written description of the data flows. The diagram(s) must:

* clearly identify anywhere State data is to be processed, stored, or transmitted;
* clearly delineate how data comes into and out of the system boundary;
* 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-2, SC-7]

Assess and describe the strength of the physical and/or logical separation measures that are inherent in the solution, or that should be configured to provide segmentation and isolation of system components and functions, addressing user-to-system; admin-to-system; and system-to-system relationships, as applicable.

The Vendor must base the assessment of separation measures on very strong evidence, such as 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.

# 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 3.2, *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 3-1. 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? |  |  |
| 2 | Does the VENDOR have the ability to consistently remediate High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days? |  |  |
| 3 | All operating systems (OS) AND major application software components (e.g. Microsoft SQL, Apache Tomcat, Oracle Weblogic, etc.), must NOT be past N-1. Applications which are not operating on the most recent platform MUST have a roadmap to upgrade with a State approved timeline. Does the application support the N-1 requirement?  |  |  |

## 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.

* + 1. 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 3-2. 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] |  |  |  |  |  |  |
| 2 | Transmission [SC-8 (1), SC-12, SC-12(2, 3)] |  |  |  |  |  |  |
| 3 | Remote Access [AC-17 (2)] |  |  |  |  |  |  |
| 4 | Authentication [IA-5 (1), IA-7] |  |  |  |  |  |  |

* + 1. Transport Layer Security [NIST SP 800-52, Revision 1]

The Vendor must identify all protocols that are used by the solution. The Vendor may add rows to the table if appropriate, but must not remove the original rows.

Table 3-3. 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) |  |  |  |
| 2 | TLS 1.0 (Non-Compliant) |  |  |  |
| 3 | TLS 1.1 (Non-Compliant) |  |  |  |
| 4 | TLS 1.2 (Compliant) |  |  |  |

* + 1. 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 3-4. Identification and Authentication, Authorization, and Access Control

| **#** | **Question** | **Yes** | **No** | **Describe capability, supporting evidence, and any missing elements** |
| --- | --- | --- | --- | --- |
| 1 | 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)] |  |  |  |
| 2 | Does the system allow for multi-factor authentication (MFA) for administrative accounts and functions? [IA-2] |  |  |  |
| 3 | Are role-based access used, managed and monitored? [IA-4/ IA-5] |  |  |  |
| 4 | Does the system restrict non-authorized personnel’s access to resources? [AC-6(2)] |  |  |  |
| 5 | Does the system restrict non-privileged users from performing privileged function? [AC-6] |  |  |  |
| 6 | 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] |  |  | The capability description is not required here, but must be included in Section 2.2, Separation Measures. |
| 7 | Does the solution enforce the State’s password policy? State requires minimum 8-character complex passwords (Upper, Lower, Special Character and Numerical), including minimum password life? [IA-5] |  |  |  |
| 8 | Does the solution require a non-user service account to function? [IA-5] |  |  |  |
| 9 | Does the solution obscure feedback of authentication information? [IA-6] |  |  |  |
| 10 | Does the solution limit unsuccessful login attempts? [AC-7] |  |  |  |
| 11 | Does the solution support a fail-safe function to deny access if the system is not functioning properly? [AC-17] |  |  | If yes, what is the limit? Can it be configured? |
| 12 | Does the solution store and forward passwords in encrypted form? [SC-8] |  |  |  |

* + 1. 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 3-5. Audit, Alerting, Malware, and Incident Response

| **#** | **Question** | **Yes** | **No** | **Describe capability, supporting evidence, and any missing elements** |
| --- | --- | --- | --- | --- |
| 1 | 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] |  |  |  |
| 2 | Does the solution log and monitor access to it? [SI-4] |  |  |  |
| 3 | 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] |  |  |  |
| 4 | Does the VENDOR have the capability to 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-11] |  |  |  |

* + 1. 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 3-6. Configuration and Risk Management

| **#** | **Question** | **Yes** | **No** | **Describe capability, supporting evidence, and any missing elements** |
| --- | --- | --- | --- | --- |
| 1 | Does the VENDOR follow a formal change control process that includes a security impact assessment? [CM-3, CM-4] |  |  |  |
| 2 | Does the solution support the ability to prevent unauthorized changes to the system? [CM-5] |  |  |  *If “yes,” describe how this is accomplished.* |
| 3 | Does the VENDOR support configuration settings for products employed that reflect the most restrictive mode consistent with operational requirements? [CM-6] |  |  |  If “yes,” describe if the configuration settings are based on Center for Internet Security (CIS) Benchmarks or United States Government Configuration Baseline (USGCB), or “most restrictive consistent with operational requirements.” |
| 4 | Does the VENDOR demonstrate the capability to remediate High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days? [RA-5, *State Continuous Monitoring policy*] |  |  | Describe how the Vendor validated that the VENDOR remediates High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days. |
| 5 | When a High vulnerability is identified as part of ConMon activities, does the VENDOR consistently check audit logs for evidence of exploitation? [RA-5] |  |  |  |

## Additional Capability Information

State will evaluate the responses in this section on a case-by-case basis relative to a State-Ready designation decision.

* + 1. 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 3-7. 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)? |  |  |  |
| 2 | Does the VENDOR have and use development and/or test environments to verify changes before implementing them in the production environment? |  |  |  |

* + 1. System and Services Acquisition

Vendors are also responsible for meeting the applicable System and Services Acquisition controls as defined in SA-4, SA-10 & SA-11.