Board Member
Powers and Duties

Tracy Doaks
Secretary and State CIO
Board Member Powers and Duties

(1) To advise the State CIO on policies and procedures to develop, review, and update the State Information Technology Plan.

(2) To establish necessary committees to identify and share industry best practices and new development and to identify existing State information technology problems and deficiencies.

(3) To establish guidelines regarding the review of project planning and management, information sharing, and administrative and technical review procedures involving State-owned or State-supported technology and infrastructure.

(4) To establish ad hoc technical advisory groups to study and make recommendations on specific topics, including work groups to establish, coordinate, and prioritize needs.
Powers and Duties (continued)

(5) To assist the State CIO in recommending to the Governor and the General Assembly a prioritized list of enterprise initiatives for which new or additional funding is needed.

(6) To recommend business system technology projects to the Department and the General Assembly that meet the following criteria:
   a. A defined start and end point.
   b. Specific objectives that signify completion.
   c. Designed to implement or deliver a unique product, system, or service pertaining to business system technology.

(7) To develop and maintain a five-year prioritization plan for future business system technology projects.
Ethics Awareness, Conflict of Interest Reminder, Public Records

Anna Szamosi
Deputy General Counsel
Ethics Awareness

- Ethics Act
  - As of today, this board is not covered by the Ethics Act
  - If the Commission does determine that this board is covered by the Ethics Act, all members will be required to complete a Statement of Economic Interest (SEI) and Ethics training, if you have not already.

- Regardless, the proposed bylaws also prohibit members from participating in discussions or votes where you may have a conflict of interest
Public Meetings

• All official meetings of public bodies are open to the public
• Official meetings for this board commence when a quorum of members is met
• Meetings can be closed for certain reasons, including when the board needs to discuss confidential information, confidential IT procurement bids, and so forth
• DIT staff will assist with required notice and posting requirements for the board
Public Records

"Public record" or "public records" shall mean all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions.

• Public records are the property of the people of North Carolina
• Unless an exception applies, NCDIT must turn over records to anyone who makes a request
• This includes emails, text messages, voicemail recordings and transcripts, etc.
• Any emails, texts, notes, etc. created in connection with your duties as a member of this board will likely be considered a public record
Exceptions to the Public Records Act

• Communications of an attorney to an agency or board regarding pending litigation or processing where the agency is a party to or is directly affected by the litigation or proceeding
• Trade secrets (intellectual property, vendor customer lists)
• Personally identifying information
• Certain meeting minutes of closed public body meetings
• Network & security features of IT systems
• Procurement information prior to award to a vendor
• Security and risk assessment reports
Applicability to the IT Strategy Board

• Any emails, texts, notes, etc. created in connection with your duties as a member of this board will likely be considered a public record

• This includes records contained in your personal email or on personal devices created while transacting official business for the board

• If you do not already have a state-issued email account, NCDIT can issue you one to use for board purposes
Board Member Service Requirement

• Per the Office of State Human Resources, all members of state boards and commissions are considered temporary state employees, even if they are not paid

• All members who are not already state employees must complete an application form and an Employment Eligibility Verification form (I-9)
  • The I-9 form requires copies of ID, SSN card, etc.
  • Bring documentation to next meeting. A representative from OSHR will be in attendance to collect this information.
Review Draft Bylaws for Consideration

Anna Szamosi
Deputy General Counsel
IT Strategy Board Bylaws

• G.S. 143B-1337 requires that the board establish bylaws that contain rules governing your meeting procedures
• Please review the bylaws that will be provided to you, and provide feedback by the end of March
Overview of the Draft Bylaws

• **Article 1:**
  - Name
  - Purpose
  - Membership of the Board

• **Article 2:**
  - Powers & duties
  - Chair & vice-chair
  - Member service
  - Meeting logistics

• **Article 3:**
  - Committees

• **Article 4:**
  - Ad hoc technical advisory groups

• **Article 5:**
  - Amendments
Questions?
Introduction to NCDIT

Tracy Doaks
Secretary and State CIO
Who We Are

**Mission:** To promote a stronger North Carolina that connects customers, citizens, business, education and government

**Purpose:** To innovatively unite business and IT to meet the needs of our citizens by delivering shared services to state agencies, local governments, and educational institutions across the state
Who We Are
Our History

• 1983 - created as the State Information Processing Services in the Office of State Controller

• 1997 - moved to the Department of Commerce, then to the Office of the Governor as the Office of Information Technology Services.

• 2015 - established in legislation as a cabinet-level department to unify state IT resources to gain efficiencies
Unifying IT Resources

• Completing in two phases
• Phase I
  • Transition IT employees under the operational control of NCDIT
  • Employees will remain in their current physical locations
  • HR actions, activities and decisions are responsibility of NCDIT upon the date of transfer
Unifying IT Resources

• Nine agencies transferred to date
  • Transportation
  • Public Safety
  • Environmental Quality
  • Military and Veterans Affairs
  • Administration
  • Cultural and Natural Resources
  • Office of the Governor
  • Budget and Management
  • Human Resources
Unifying IT Resources

• Phase II
  • Will focus on analysis of business operations and processes to ensure the most effective and efficient use of IT resources
  • NCDIT will also assume full budgetary authority of the positions through the implementation of a new fiscal model
VISION: A CULTURE OF INNOVATION AND OPERATIONAL EXCELLENCE

COLLABORATION BETWEEN STATE AND LOCAL GOVERNMENT
Forge strong partnerships with local governments and build awareness of available NCDIT resources, including IT procurement, shared services and cybersecurity tools.

DIGITAL TRANSFORMATION
Leverage digital technology to make government services more accessible and interactive to achieve better outcomes for our customers and residents.

CYBERSECURITY
Continue to be a leader in cybersecurity through a whole-of-state approach that protects the state, its residents and their data.

BROADBAND
Ensure all North Carolinians have access to an affordable high-speed internet connection anytime, anywhere.

WORKFORCE
Invest in our people to ensure we have the necessary skills to be agile and adapt to changing technology and business needs.

This investment also will allow us to recruit and retain talented people with a passion to innovate and serve.
Service Delivery and IT Solutions

Glenn Poplawski
State Solutions Director
Enabling Digital Transformation

Benefits for Citizens

- Simpler, faster, more intuitive experiences with state government.
- Transparent, open, accessible government
- Security and privacy

Benefits for State Government

- Cost savings and efficiencies
- Decreased call center volume and fewer office visits
- Engaged, productive staff
- Better positioned for workforce of the future

Learn more: DIT IT Plan: https://it.nc.gov/roadmap
Cybersecurity

Maria Thompson
State Risk Officer
Enterprise Security and Risk Management Office (ESRMO)

Mission

Provides leadership in the development, delivery and maintenance of an information security and risk management program that safeguards the state's information assets and the supporting infrastructure against unauthorized use, disclosure, modification, damage or loss.
ESRMO

- Supports a comprehensive statewide program that encompasses information security implementation, monitoring, threat and vulnerability management, cyber incident management and enterprise business continuity management.
- Works with executive branch agencies to help them comply with legal and regulatory requirements, the statewide technical architecture, policies, industry best practices, and other requirements.
- Works with state agencies, federal and local governments, citizens and private-sector businesses to help manage risk to support secure and sustainable IT services to meet the needs of North Carolinians.
Why is Cybersecurity Important?

Key component of any risk management strategy
• State and local government IT struggle with obtaining and building it into business requirements
• Shadow IT activities are prevalent throughout the state
• State agencies, local government and academia are resource constrained – lack of manpower
  • Local county networks host critical services for the state
    o Critical infrastructure, e.g. elections, water, power etc.
    o Life and safety services, e.g. 911, health, public safety
• Current decentralized cyber practices, ad hoc cyber budgeting and lack of accountability for cyber risks leads to inconsistent cyber approach and poor risk management
  • Limited network visibility
  • Legacy systems with no maintenance or patch support
  • Ineffective identity, credential and access management
  • Slow incident response capabilities
## Strategic Objectives

<table>
<thead>
<tr>
<th>Key Initiatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Develop, implement and fund a statewide cyber incident response capability to support secure citizen engagements</td>
</tr>
<tr>
<td>• Reduce the risks to the state’s critical infrastructure by collaborating with local government</td>
</tr>
<tr>
<td>• Advance the state’s cyber workforce through education and collaboration with K-12 and higher education</td>
</tr>
<tr>
<td>• Protect and secure statewide government and academic networks</td>
</tr>
<tr>
<td>• Assess, trend and evaluate emerging cyber risks to the state</td>
</tr>
<tr>
<td>• Support federal and state partners in combatting cybercrime targeting citizens and small businesses</td>
</tr>
<tr>
<td>• Establish a statewide privacy program to address growing concerns on data management practices</td>
</tr>
</tbody>
</table>
Whole-of-State Cyber Approach

Eliminating all risks is virtually impossible—unifying cyber, managing risks and building resilience will be the key to a more secure state!

- BitSight monitoring of local county infrastructure
- Pilot program for continuous monitoring of local county network traffic
- Developed of Statewide Significant Cyber Incident Plan
- Established statewide information sharing under HB 217
- Cyber incident response and training support utilizing National Guard Defensive Cyber Operations team and local IT Strike teams
## NC Reported Ransomware Attacks

<table>
<thead>
<tr>
<th>Date</th>
<th>Affected Entity</th>
<th>Ransomware /Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb. 2016</td>
<td>Durham</td>
<td>Unknown</td>
</tr>
<tr>
<td>Dec. 2017</td>
<td>Mecklenburg County</td>
<td>LockCrypt</td>
</tr>
<tr>
<td>Feb. 2018</td>
<td>Davidson County</td>
<td>SamSam</td>
</tr>
<tr>
<td>May 2018</td>
<td>Pasquotank County</td>
<td>Scarab</td>
</tr>
<tr>
<td>Oct. 2018</td>
<td>Onslow County Water and Sewer</td>
<td>Ryuk</td>
</tr>
<tr>
<td>Nov. 2018</td>
<td>City of Durham</td>
<td>Unknown</td>
</tr>
<tr>
<td>March 2019</td>
<td>Orange County (hit 3 times in 6 yrs)</td>
<td>Ryuk</td>
</tr>
<tr>
<td>March 2019</td>
<td>Pasquotank-Camden EMS</td>
<td>Unknown</td>
</tr>
<tr>
<td>March 2019</td>
<td>Robeson County</td>
<td>Ryuk</td>
</tr>
<tr>
<td>April 2019</td>
<td>City of Greenville</td>
<td>RobinHood</td>
</tr>
<tr>
<td>July 2019</td>
<td>Richmond Community College</td>
<td>Ryuk</td>
</tr>
<tr>
<td>Aug. 2019</td>
<td>Lincoln County Sheriffs Office/911 (X2)</td>
<td>DopplePaymer</td>
</tr>
<tr>
<td>Sept. 2019</td>
<td>NC Wildlife Resources Commission</td>
<td>DopplePaymer</td>
</tr>
<tr>
<td>Oct. 2019</td>
<td>NC State Bar</td>
<td>Neshtya (dropper)</td>
</tr>
<tr>
<td>Oct. 2019</td>
<td>Columbus County School System (x17)</td>
<td>Ryuk</td>
</tr>
<tr>
<td>Oct. 2019</td>
<td>ABC Board (x21)</td>
<td>Sodinokibi</td>
</tr>
<tr>
<td>Dec. 2019</td>
<td>EBCI</td>
<td>Sodinokibi (Insider Threat)</td>
</tr>
<tr>
<td>Jan. 2020</td>
<td>Duplin County</td>
<td>Ryuk</td>
</tr>
</tbody>
</table>
Govt Supporting Govt – NC National Guard

20-001 Statewide Cyber Assessment
- DIT Funded - 10 Soldier Cyber Assessment and Assist Team
- Prioritize Assessing 40 Tier 1 Counties until 01JUL2020

Focus:

Concept of Operations:
- Scope: Schedule, SOW, Rules For the Use of Cyber
- Assess: Hands on Onsite Assessment, Executive and Technical Reports
- Train: Remediation Training

End State:
Allow the counties to “See Themselves” from a cyber risk perspective
“Train” the counties in remediation techniques from assessment findings
Understand the total threat landscape across NC counties

Assessments (Completed \ Scheduled)
West – 2 \ 4
Central – 4 \ 7
East – 9 \ 7

* Schedule completely full through MAY

Category I Finding:
Definition: allow primary security protections to be bypassed if compromised
Per location: CAT I findings
Total: CAT I findings
Bottom Line: Exploits developed and available

Category II Finding:
Definition: potential to lead to unauthorized system access
Per location: CAT II findings
Total: CAT II findings
Bottom Line: Exploit development required
Continuous Monitoring & Annual Compliance Reporting

• N.C.G.S. 143B-1376 requires the State CIO to annually assess the ability of each agency and their contracted vendors to comply with the current enterprise-wide set of security standards. The information gathered is used to build out the State IT Plan. These assessments include, at a minimum:
  
  1. Rate of compliance with the enterprise-wide security standards
  2. Estimate of cost to implement deficient security measures
  3. Assessment of Security Organization
     • Security practices
     • Security industry standards
     • Network security architecture
     • Current expenditures of state funds for IT security

• ESRMO has developed a Continuous Monitoring Plan that requires all agencies to complete an annual risk and security assessment and have ongoing processes in place to assess the current posture of the environment.
  
  • All critical systems must obtain a third-party assessment within a 3-year cycle. In the off-years, agencies conduct an annual self assessment.
General Discussion & Q & A
NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

VISION: A CULTURE OF INNOVATION AND OPERATIONAL EXCELLENCE

COLLABORATION BETWEEN STATE AND LOCAL GOVERNMENT
Forge strong partnerships with local governments and build awareness of available NCDIT resources, including IT procurement, shared services and cybersecurity tools.

DIGITAL TRANSFORMATION
Leverage digital technology to make government services more accessible and interactive to achieve better outcomes for our customers and residents.

CYBERSECURITY
Continue to be a leader in cybersecurity through a whole-of-state approach that protects the state, its residents and their data.

BROADBAND
Ensure all North Carolinians have access to an affordable high-speed internet connection anytime, anywhere.

WORKFORCE
Invest in our people to ensure we have the necessary skills to be agile and adapt to changing technology and business needs.

This investment also will allow us to recruit and retain talented people with a passion to innovate and serve.