Meeting Notice & Agenda:
Florida Cybersecurity Task Force

Date, Time & Location:
October 22, 2019
3:00PM-5:00PM
301 Senate Office Building
400 South Monroe Street
Tallahassee, FL 32399

I. Call to Order

II. Roll Call

III. Member Introductions

IV. Review and Adoption of Task Force Rules

V. Presentation: Scope, Purpose, and Responsibility of the Task Force

VI. Presentation: State of our Cybersecurity Infrastructure

VII. Presentation: Government in the Sunshine Training

VIII. Other Business & Proposed Meeting Schedule

IX. Public Testimony

X. Adjournment
PROPOSED SCOPE AND SCHEDULE

TASK FORCE PRIORITIES:

1) Communicate a sense of urgency on the importance of protecting citizen’s data and personal information through increased awareness and a renewed commitment to information security.

2) Coordinate with industry leaders who may provide additional insight beyond the scope of state government and current operations.

3) Required objectives: utilize proactive measures to counteract cyberthreats including collaborative partnerships, strategic planning, the research and drafting of best practices, and adherence to the following objectives:
   a. Recommend methods to secure the state's network systems and data, including standardized plans and procedures to identify developing threats and to prevent unauthorized access and destruction of data.
   b. Identify and recommend remediation, if necessary, of high-risk cybersecurity issues facing state government.
   c. Recommend a process to regularly assess cybersecurity infrastructure and activities of executive branch agencies.
   d. Identify the current condition of the state's overall cybersecurity infrastructure, governance, and current operations. Based on any findings of deficiencies, the task force shall make recommendations for improvement.
   e. Recommend cybersecurity improvements for the state's emergency management and disaster response systems.
   f. Recommend cybersecurity improvements of the state data center.
   g. Review and recommend improvements relating to the state's current operational plans for the response, coordination, and recovery from a cybersecurity attack.

4) Strategic topics: provide opportunities for discussion related to additional policy-area specific improvement opportunities including:
   a. Intergovernmental Coordination (State-Local-Federal) & Elections
   b. Education
   c. Commerce, Transportation & Tourism
   d. Healthcare
   e. Emergency Management & Response
   f. Government Accountability & Auditing
   g. Financial Services
   h. Sensitive Information & Law Enforcement (Personal, CJIS & HIPPA)

5) Cover a specific strategic focus area and required objective at each meeting.
ARTICLE I: NAME
As specified in Chapter 2019-118, Laws of Florida the Task Force shall be named the Florida Cybersecurity Task Force (Task Force).

ARTICLE II: PURPOSE & SCOPE
The Task Force is created adjunct to the Department of Management Services to review and assess Florida’s cybersecurity infrastructure, governance, and operations. The Task Force is required to operate in a manner consistent with s. 20.052, F.S. The responsibilities and duties of the Task Force will be in accordance with Florida Statutes.

This Task Force is charged to analyze the current state and potential for improvement in the security program of state government and that of the individual agencies and prioritizing the risks posed by identified threats. The expected result is a report defining additions to current technologies, processes, and personnel necessary to close shortfalls, mitigate risk, and protect the data of Florida’s citizens.

The Task Force shall identify the best practices and standards to improve the protection of the data entrusted to the State of Florida by its citizens. The Task force will diligently perform the tasks set forth by the legislature to identify cybersecurity gaps, remediation needs, and infrastructure improvements within the State of Florida enterprise. The scope of this Task Force includes conducting conversations with public, private, and thought leaders in a series of collaborative meetings to build consensus among experts from within and out of state government. These activities should include opportunities to hear from and recommend options to assist local governments.

ARTICLE III: RESPONSIBILITIES
As referenced in Chapter 2019-118, Laws of Florida the Task Force must complete the following:

1. Recommend methods to secure the state's network systems and data, including standardized plans and procedures to identify developing threats and to prevent unauthorized access and destruction of data.
2. Identify and recommend remediation, if necessary, of high-risk cybersecurity issues facing state government.
3. Recommend a process to regularly assess cybersecurity infrastructure and activities of executive branch agencies.
4. Identify the current condition of the state’s overall cybersecurity infrastructure, governance, and current operations. Based on any findings of deficiencies, the Task Force shall make recommendations for improvement.
5. Recommend cybersecurity improvements for the state's emergency management and disaster response systems.
6. Recommend cybersecurity improvements of the state data center.
7. Review and recommend improvements relating to the state's current operational plans for the response, coordination, and recovery from a cybersecurity attack.
In accordance with Chapter 2019-118, Laws of Florida, this Task Force is required to submit a report of its findings and recommendations to the Governor, the President of the Senate, and the Speaker of the House of Representatives on or before November 1, 2020.

In addition to the requirements specified above, the Task Force shall include recommendations to assist local governments as part of the final report.

Finally, the Task Force may also submit interim recommendations as approved by a majority vote to the interested parties specified above.

**ARTICLE IV: MEMBERSHIP**

**Section 1- Composition**
As specified in law, membership in this Task Force is limited to the following:

- The Lieutenant Governor, or his or her designee to serve as Chair of the Task Force
- A representative of the Florida Computer Crime Center within the Florida Department of Law Enforcement (FDLE)
- A representative of the Florida Fusion Center within the FDLE
- The State Chief Information Officer
- The State Chief Information Security Officer
- A representative of the Division of Emergency Management within the Executive Office of the Governor
- A representative of the Office of the Chief Inspector General in the Executive Office of the Governor
- A member appointed by the President of the Senate
- A member appointed by the Speaker of the House of Representatives
- Members of the private sector appointed by the Governor

**Section 2- Term**
- Members of the Task Force shall serve for the duration of the existence of the Task Force and shall attend meetings on a regular basis.

**ARTICLE V: OFFICERS**
As specified in law, the Lt Governor or his or her designee shall serve as Chair. If the Lt. Governor should need to delegate his or her authority for a specified meeting, the Chair may temporarily assign the duty for a specified meeting to another Task Force member for the specified meeting and would be required to be completed on a per-meeting basis.

**ARTICLE VI: MEETINGS**

**Section 1- Meeting Requirements**
As specified in law, the Task Force must meet quarterly. Meetings of the Task Force shall be called by the Chair and properly noticed, in accordance with applicable Sunshine Laws. Noticed meetings may be canceled at the Chair’s discretion.
Section 2- Meeting Notices
All meetings must be scheduled and officially advertised in advance in compliance with Florida’s Sunshine Law (Chapter 286, Florida Statutes).

Section 3- Agenda
An agenda for a properly noticed meeting shall be created by the Chair. Any changes or additions to the agenda shall be decided by a two-thirds vote of the members of the Task Force present and voting.

Section 4- Quorum
A quorum necessary for the transaction of the business of the Task Force shall consist of a simple majority of the total appointed membership as listed in Article IV. An official quorum of Task Force members must be present at the meeting for the Task Force to conduct official business.

Section 5- Use of Technology Participation Tools
The Chair may approve participation by members using technology. Members participating through technology tools may also be counted as present for the purpose of establishing a quorum as referenced in Section 3 of this Article.

ARTICLE VII: OPERATING PROCEDURES
The Chair shall decide all questions of order. The latest edition of Mason’s Manual of Legislative Procedure may be consulted, but shall not be binding, when a question of procedure is not addressed by the Florida Law, these Rules, or prior rulings.

ARTICLE VII: WORKING GROUPS
The Chair may appoint work groups to study issues and present findings and recommendations to the Task Force.

ARTICLE VIII: AMENDMENT OF THESE BYLAWS
These bylaws may be amended at any regular meeting of the Task Force by a two-thirds vote, provided that the amendment has been submitted in writing at the previous regular meeting. These bylaws and all amendments there to shall become effective on the date of Task Force approval.
Bill Summary

• Merged the Agency for State Technology into the DMS Division of Telecommunications to create the Division of State Technology

• Established the State Chief Information Officer reporting to the DMS Secretary

• Established a “Cloud-First” policy for state agencies

• Created the Florida Cybersecurity Task Force led by Lt. Governor Nuñez to study cybersecurity procedures, rules, and vulnerabilities and make recommendations

• Encourages the conversation of data-interoperability between agencies
Merger of AST into DMS

Initial Transition
- All FTE’s transferred on July 1, 2019
- Positions continue to be updated to reflect organizational changes
- Organizational assessment underway

State Chief Information Officer
- National search for State CIO
- Final interviews underway, expected to be complete by early 2nd quarter
Strategic Priorities

- Cloud Computing
- Cybersecurity
- Data Interoperability
Cloud-First Policy

Policy Overview
• Creates a cloud-first policy for state agencies, requiring each agency to first consider cloud computing solutions when sourcing technology

• Requires DMS to establish best practices for the procurement of cloud computing services

• Requires DMS to appoint a State Data Center Director who has experience in leading data center facilities and cloud computing management

Cloud Rulemaking
• Collaborative process to provide guardrails

• Robust public comment with over 100 workshop participants
Creating Efficiencies

Business Case
• The Department is currently in the process of procuring an independent consultant to conduct a business case.
• The business case will examine options of how best to operate the state data center in full support of the cloud-first strategy.
• The Department will report the findings to the Governor and Legislature for consideration.

Application Strategic Plan
• Due by October 15, 2019 to be updated annually by each state agency
• Provides inventory of applications at the State Data Center
• Plan must identify an approximate timeline and readiness of transitioning to the cloud
• The State Data Center should utilize information from state agencies’ strategic plans when determining services.
Data Interoperability

Overview

• Legislation requires DMS to recommend potential methods for standardizing data across state agencies that will promote interoperability and reduce the collection of duplicative data.

Benefits of Interoperability

• Provide connections across policy silos
• Allows for decision makers to reference trends that may lead to better outcomes or cost-savings
• Improve customer service
Protecting Florida’s Data

Cybersecurity

• State Chief Information Security Officer (CISO) is established to provide a strategic vision and plan for the enterprise

• Continued coordination with the Department of Homeland Security and the State University System

• Development of Florida’s Cyber Disruption plan in coordinating with FDLE, DEM, and the National Guard

• Updated Agency guidance to reflect the increase in intellectual threats

• Support government entities with best practices related to Cybersecurity protocols.
  • October is Cybersecurity Awareness Month
Cybersecurity Task Force

• The Task Force was established to review and assess Florida’s cybersecurity infrastructure, governance, and operations.

• The Task Force will analyze the state of our current cybersecurity infrastructure and operations and recommend different potential areas for improvement.

• Recommendations should include short and long term solutions aimed at key objectives.

• Provide opportunities for discussion related to additional policy-area specific improvement opportunities.
Required Objectives

• Recommend methods to secure the state's network systems and data, including standardized plans and procedures to identify developing threats and to prevent unauthorized access and destruction of data.

• Identify and recommend remediation, if necessary, of high-risk cybersecurity issues facing state government.

• Recommend a process to regularly assess cybersecurity infrastructure and activities of executive branch agencies.

• Identify the current condition of the state's overall cybersecurity infrastructure, governance, and current operations. Based on any findings of deficiencies, the task force shall make recommendations for improvement.
Required Objectives

• Recommend cybersecurity improvements for the state's emergency management and disaster response systems.

• Recommend cybersecurity improvements at the state data center.

• Review and recommend improvements relating to the state's current operational plans for the response, coordination, and recovery from a cybersecurity attack.
Strategic Topics

- Intergovernmental Coordination & Elections
- Education
- Commerce, Transportation & Tourism
- Healthcare
- Emergency Management & Response
- Government Accountability & Auditing
- Financial Services
- Sensitive Information & Law Enforcement
Path Forward

• Communicate a sense of urgency on the importance of protecting citizen’s data and personal information through increased awareness and a renewed commitment to information security.

• Coordinate with industry leaders who may provide additional insight beyond the scope of state government and current operations.

• Meetings occur once every one-to-two months at locations throughout the state which will allow the Task Force to hear from stakeholders across policy areas.
QUESTIONS?
State of our Cybersecurity Infrastructure
The Cyber Mission

- Department of Management Services
  - Division of State Technology
    - Bureau of State Information Security
  - State Chief Information Security Officer
    - Strategic Security
    - Security Operations
The Cyber Mission

Strategic Security

- Maintain Rule 60GG-2 – The Florida Cybersecurity Standards (FCS)
- Coordinate enterprise security training
- Liaise with law enforcement and external cyber-intelligence partners
- Review agency legislative requests to validate cybersecurity components
- Monitor incident reports for multi-agency response coordination
- Collect and analyze statutorily required agency assessments
The Cyber Mission

Security Operations

• Provide cybersecurity capabilities for the State Data Center
• Assist incident monitoring and response for customer agencies
• Manage security tools for datacenter resources
• Provide security guidance in system development and deployment
• Scan customer systems for known vulnerabilities
State Chief Information Security Officer

282.318 Florida Statutes defines the position of State Chief Information Security Officer (CISO):

3) ...The department shall ... (a) Designate a state chief information security officer who must have experience and expertise in security and risk management for communications and information technology resources.

Thomas Vaughn, CISSP, CEH
Incumbent since December 2017
Information Technology Security Act - 282.318 F.S.

Statutory Mandates
1. Establish standards and processes for information technology security
2. Adopting rules that safeguard an agency’s data, information, and information technology resources
3. Designate a state chief information security officer
4. Develop a strategic statewide cybersecurity plan
5. Publish an information technology security framework for state agency use
6. Establish asset management procedures
7. Support operational risk decisions using a standard risk assessment methodology
Information Technology Security Act - 282.318 F.S.

Statutory Mandates

8. Use information from detection and response activities to inform agency cybersecurity incident response plans

9. Develop strategic and operational information technology security plans

10. Establishing the managerial, operational, and technical safeguards to protect

11. Assist state agencies comply with 282.318

12. Provide training for state agency information security managers and computer security incident response team members

13. Review the strategic and operational information technology security plans of executive branch agencies
Florida Cybersecurity Standards (FCS) - Rule 60GG-2

The FCS is based on the NIST Cybersecurity Framework (CSF) and is in synch with the CSF version 1.1.

<table>
<thead>
<tr>
<th>Function Identifier</th>
<th>Function</th>
<th>Category Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.SC</td>
<td>Supply Chain Risk Management</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Identity Management and Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>
2018-2021 Statewide IT Strategic Security Plan

• **Strategy 1: Improve Foundational Cybersecurity Resources**
  • Objective 1: Florida Cybersecurity Framework Guidance and Improvement Development
  • Objective 2: Train Personnel and Grow Cybersecurity Skillsets
  • Objective 3: Cultivate Partnerships for Response Efforts

• **Strategy 2: Enhance Situational Awareness**
  • Objective 1: Foster Collaboration and Encourage Information Sharing
  • Objective 2: Develop Strategic Framework for Intelligence Analysis
  • Objective 3: Establish Tools and Resources to Identify Threats and Collect Intelligence

• **Strategy 3: Continually Harden the Environment**
  • Objective 1: Minimize Vulnerabilities
  • Objective 2: Develop Data Asset Tracking
  • Objective 3: Implement Appropriately Hardened System Configurations
Current Initiatives

• Cybersecurity Training
  • Agency cybersecurity professional development
  • Enterprise phishing and security awareness training

• Cybersecurity Task Force

• Elections Cybersecurity

• DHS Cyber Storm 2020 Exercise
Concept: Statewide Cybersecurity Operations Center (CSOC)
Questions?

Thomas Vaughn
Chief Information Security Officer
(850) 412-6053
thomas.vaughn@dms.myflorida.com
Florida Sunshine Law Overview
Public Meetings & Public Records
OVERVIEW

Meetings of public boards or commissions must be open to the public;

Reasonable notice of such meetings must be given; and

Minutes of the meetings must be taken, promptly recorded, and open to public inspection.
SCOPE OF THE SUNSHINE LAW

- Board members may not use the telephone, Facebook, email, or text messages to conduct a private discussion about board business.

- While a board member is not prohibited from discussing board business with staff or a non-board member, these individuals cannot be used as a liaison to communicate information between board members. For example, a board member cannot ask staff to poll the other board members to determine their views on a board issue.

- The Sunshine Law provides that no resolution, rule, regulation, or formal action shall be considered binding except as taken or made at an open meeting.

- If you receive a communication regarding the task force, specifically soliciting an idea or process, reach out to the board’s staff for guidance.

- Penalties can be levied for violations, including misdemeanors and fines.
SCOPE OF THE SUNSHINE LAW

• It provides a right of access to governmental proceedings at both the state and local levels.

• The law is equally applicable to elected and appointed boards.

• It has been applied to any gathering of two or more members of the same board to discuss some matter which will foreseeably come before that board.

• Advisory boards created are subject to the Sunshine Law, even though their recommendations are not binding upon the agencies that create them.
WHAT IS A PUBLIC RECORD?

• “All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission.”

• “…made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency…”

• That is “intended to perpetuate, communicate, or formalize knowledge of some type.”
  
  • Communicate Knowledge – share/exchange/pass-on/impart/convey/transmit
  • Formalize Knowledge – to give a certain or definite form; to shape
  • Perpetuate Knowledge – to cause the knowledge to last indefinitely
WHAT IS NOT A PUBLIC RECORD?

Documents that are NOT intended to perpetuate, communicate, or formalize knowledge of some type.

• Includes documents that are not intended as final evidence of the knowledge to be recorded.

• Personal notes such as handwritten notes that are “merely preliminary materials” intended to aid in the creation of a document that is later formalizing knowledge.

• Personal notes to yourself which are designed for your own personal use in remembering certain things.

• These only include those documents that serve no governmental function.
NOTES & DRAFTS

Be careful of your notes and drafts.

Documents and Records are considered public if they are used to “perpetuate, communicate, or formalize knowledge.”

“When-in-doubt”, check with the Task Force attorney before making a decision to disclose your documents and records.
EXEMPTIONS AND CONFIDENTIALITY

• All public records must be open for inspection and copying by any person except if they have been limited in some way by the legislature.

• The legislature has enacted statutes that have general exemptions and confidentiality provisions that prevent certain types of records from being inspected or copied.

  • These appear in Chapter 119, F.S., and other statutes.

  • These can also be program or division specific.
PUBLIC RECORDS INFORMATION

• Expect everything to be a public record.

• Before you send anything, consider it could end up on the front page of the New York Times.

• Best Practice: Don’t mix work and pleasure when emailing and texting.

• Just because it is an exchange between you and your attorney, there is no guarantee the attorney-client privilege protects it.

• If you get a question or request for a public record, see the board’s public record liaison.
QUESTIONS OR CONCERNS?

When in doubt or if you have questions:

• Look it up in Chapter 119, Florida Statutes (or other governing statutes and rules)

• Look it up in the Government-In-Sunshine Manual (the current year’s edition)

• Speak to your board attorney or ethics attorney:

  Chasity O’Steen
  Chasity.Osteen@DMS.myflorida.com

  Sean Gellis
  Sean.Gellis@DMS.myflorida.com