

### GUEST SPEAKERS



**Jamie Grant**  
State of Florida Chief  
Information Officer



**Chris Cruz**  
Former County Chief  
Information Officer and  
Public Sector CIO,  
Tanium

## INTRODUCING THE STATE OF FLORIDA CYBERSECURITY GRANT PROGRAM FOR LOCAL GOVERNMENTS

Register Here!



**ONLINE**

**WEBINAR**

**Tuesday, January 31, 2023**  
**11:30 AM**




1

# INTRODUCING THE STATE OF FLORIDA CYBERSECURITY GRANT PROGRAM FOR LOCAL GOVERNMENTS



2

## 2022 Legislation

Two bills—FAC Supported & **PASSED**

- HB 7055—Cybersecurity Reporting, Standards, and Training for Local Governments
  - [s. 282.3185, Florida Statutes](#)
- HB 7057—Public Records Exemption for Critical Infrastructure and Cybersecurity Information
  - [s. 119.0725, Florida Statutes](#)

3

## HB 7057—Public Records & Meetings/Cybersecurity

- General public record exemption or public meeting exemption related to state or local government cybersecurity information
  - Coverage limits
  - Network schematics, hardware and software configurations
  - Cybersecurity incident information
  - Public Meetings exemption

4

## HB 7055 — Cybersecurity

- Ransomware Prohibition
- Incident reporting requirements
- Standards adoption
- Training for State & Local Governments
- Uniform compliance across state and local agencies
- **FUNDED** mandate

5

Florida [Digital Service]

# CYBERSECURITY OPERATIONS

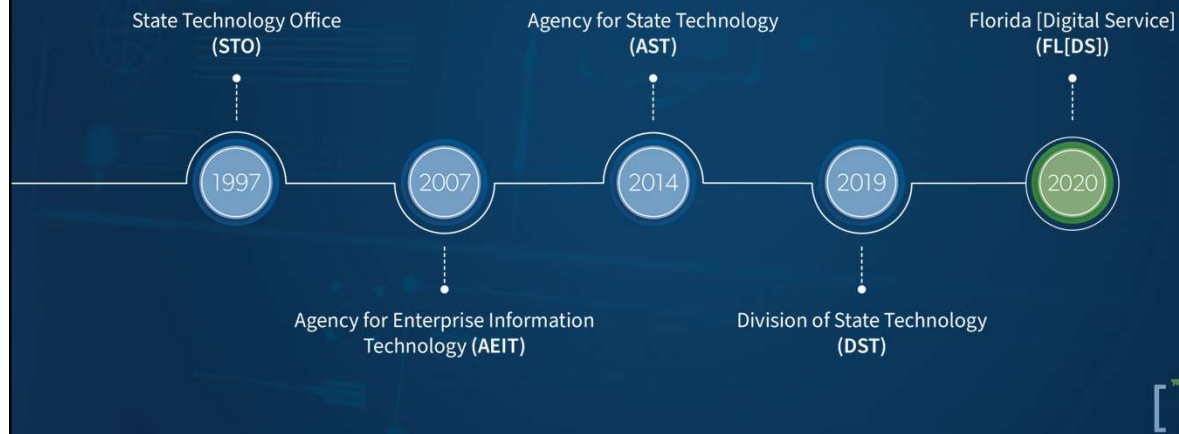
2023\_JANUARY

6

6

# The History of State Technology in Florida

So Challenged that it has Successfully Defied the Law of Bureaucracy



7

## The Costs of Not Getting it Right

Since 2005, in Florida there have been...

FIVE  
\$10 MILLION+  
canceled IT projects  
resulting in  
**\$157.4 MILLION**  
in wasted funds. <sup>1</sup>

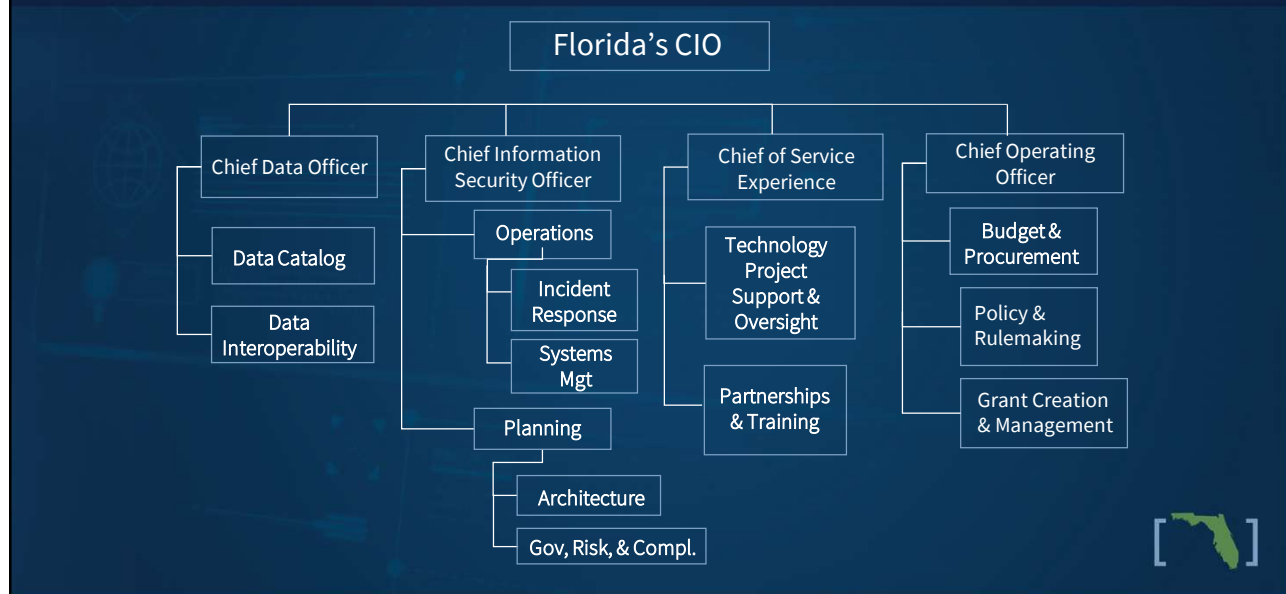
SEVEN  
\$10 MILLION+  
completed IT projects  
that went collectively  
over budget by  
**\$327.5 MILLION.** <sup>1</sup>

In 2020,  
**CYBERCRIMES**  
cost Florida  
**\$295 MILLION,** <sup>2</sup>  
which ranks  
**4<sup>th</sup>** HIGHEST IN  
THE U.S.

1. Leznoff, Joanne. 2021. "FDS- Florida Digital Service." House Government Operations Subcommittee. Florida House of Representatives.  
2. Sharton, Brenda. 2021. "Ransomware Attacks are Spiking. Is your Company Prepared?" Harvard Business Review. Available at: <https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared>

8

## The Structure of the Florida Digital Service



9

## Enterprise Cybersecurity Program

- FL[DS] serves as the lead state entity on cybersecurity. 282.318, F.S. directs the Digital Service to:
  - Operate and maintain a Cybersecurity Operations Center led by the State CISO, including a process for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents.
  - Detect threats through proactive monitoring, continuous security monitoring, and defined detection processes.
  - Establish incident response teams.
  - Recover information and data in the event of a cybersecurity incident.
  - Establish managerial, operational, and technical safeguards for protecting state government data and information technology resources, including establishing standards and processes for assessing state agency cybersecurity risk.

10

## Individual State Agency Responsibilities

- Section 282.318(4), F.S. includes requirements of each agency, including:
  - Designate an Information Security Manager (ISM), coordinate cyber training.
  - Establish an agency cybersecurity team to respond to an incident and immediately report all confirmed or suspected incidents to the State CISO.
  - Conduct, and update every 3 years, a comprehensive risk assessment, to determine the security threats to the data, information, and IT resources.
  - Submit annually by July 31, strategic and operational cybersecurity plans.
  - Implement managerial, operational, and technical safeguards and risk assessment remediation plans recommended to address identified gaps in data, information, and information technology resources of the agency.
  - Develop a process for detecting, reporting, and responding to threats, breaches, or cybersecurity incidents which is consistent with security rules, guidelines, and processes established by the Florida Digital Service.



11

## The Current Posture



Positive Increase / Decrease



Negative Increase / Decrease



No Change

### FLDS:

- Number of FTE: 70
- Cybersecurity FTE: 29
- Total FY 2022-2023 Appropriation: \$148.2M
- Total FY 2022-2023 Cybersecurity Appropriation: \$62.2M

### Agency Collaboration:

- Number of Agencies which had ever collaborated in real-time on cybersecurity prior to FLDS: 0
- Number Currently Collaborating in real time on cybersecurity with FLDS: 32
- Number of Agencies Fully Integrating with the CSOC: 9
- Number of Agencies Partially Integrating the CSOC: 23



12

## The Current Posture



Positive Increase / Decrease



Negative Increase / Decrease



No Change

### High Level Threat Data

- Total Threat Sightings for the 6 agencies which have completed the Phase 1 integration with the CSOC : >2 Million
- Total Investigations Currently Open: 172
- Open Investigations per FLDS FTE: 2.45
- Open Investigations per Cybersecurity FTE: 5.93
- Threat Sightings per FLDS FTE: 28,571
- Threat Sightings per Cybersecurity FTE: 68,966



13

## Florida's First Cybersecurity Operations Center

### Developing Security Capabilities from the Ground Up

#### Three Predominant Program Designs:

1. Single-Stack: procuring a standalone solution to operationalize all capabilities which eliminates dependence on third party integrations but limits product options.
2. Systems Integrator: procuring a single vendor to run the initiative and outsource all technology decision making to that vendor to determine design, architecture, and product roadmap (i.e., Deloitte, Accenture, KPMG, etc.).
3. Multi-Vendor Integrated Marketplace: a modular approach that supports numerous vendors and integrates multiple solutions.

FL[DS] selected #3 as the design for the CSOC for the following reasons:

- Establish a single point of ingestion, translation, and access for cybersecurity data.
- Avoid single vendor dependence.
- Provide access to the best solutions for each function.
- Avoid requiring agencies to adopt a single technology stack for all necessary functions.
- Preventing agencies from having to rip and replace certain solutions already deployed.



14

# Ending the Siloed Approach to Security

FL[DS] began by focusing on two very real threats to the enterprise:

1. Zero state agencies were sharing security data or collaborating in real time on cybersecurity.
2. Unsupported and unsecured versions of Microsoft Office were being used prominently across state government.

FL[DS] offered to fund solutions to all state agencies. Initially, 21 of 36 state agencies opted to participate:

- FL[DS] funded cloud-based Microsoft Office Suite, including cloud-based email.
- Third-party, private sector implementation services, included at no additional cost to the taxpayer.
- Microsoft included engineering support post-implementation at no additional cost to the taxpayer.
- FL[DS] generated significant savings by purchasing as an enterprise which saved 25% (\$4M) above and beyond state term contract.

FL[DS] has committed to provide these solutions to 7 additional enterprise entities which have opted in.



15

## Florida's First CSOC Launching the Core Functionalities

Building upon the focus on eliminating unsupported and unsecure productivity software, **FL[DS] deployed the core functionalities of a Cybersecurity Operations Center** including:






- **Asset Discovery** to identify and inventory enterprise technology resources:
  - Agent-based solution focused on infrastructure and supported with Managed SOC Services.
  - Agentless solution focused on network traffic and supported with managed services.
  - Internet-facing attack surface discovery.
- **Endpoint Detection and Response** to provide comprehensive and complimentary enterprise support.
- **Managed SOC Solution and Services** software which integrates all other incorporated solutions and supported by 24/7/365 Managed Security Services.
- **Content Delivery Network** to manage and secure enterprise web assets, both .com and .gov.
- **Training** Cyber range infrastructure and curriculum to support cybersecurity training and skill development.
- **Licensure and Credential Access** FL[DS] proof of concept to explore workstation licensure and credential management to ensure efficient offboarding of employees.







16






# Quantifying the Threat Landscape

  Positive Increase / Decrease  
  Negative Increase / Decrease  
 No Change

## Asset Discovery: External View

- Total On-premise Assets Discovered: 961,386 
- Total Cloud Assets Discovered: 9,018 
- Open/Critical Issues: 4,030  / 274 
- Top Threat: Insecure Web Servers (56)






## Asset Discovery: Network Sensors (last 30 days)

- Discovered Devices: 360K 
- High Risk Devices: 13.4K 
- Threat Activity: 5,600 Events 



## Asset Discovery: Endpoint Sensors (last 30 days)

- Endpoints w/ Agent Installed: 6,242 
- Discovered Devices: 10,683 
- Devices Missing Patches: 6,578  (301 Critical)

## Endpoint Detection and Response (30 Day Lookback):

- Resolved Incidents (30 days): 190 
- Threats Detected (30 Days): 192 
- Malicious Threats Mitigated (30 Days): 39 
- Closure Rate Prior 30 Day Period: 99.68% 
  - 30 day period prior was 83.52%
- Current Closure Rate: 98.95% 

## Content Delivery Network (30 Day Lookback):

- State Websites Actively Protected: 51 
- Attack Traffic Diverted: 6.4 Million Events (e.g., Botnet, DDoS) 



17

# Cyber Security Updates: Strategy and Planning – 2022 Review

- **CSOC launched**
- **State Incident Response Plan Published**
  - Living document to support state and local entities needing to report a cybersecurity incident to facilitate incident response
- **Launched Cyber Range training capabilities with real-time blue team training for security professionals to respond to an active intrusion or attack.**
  - 20+ agencies have either run or are scheduled to run exercises since September 2022 on the Cloud Range platform
- **Established Statewide Cybersecurity Strategic Plan:**
  - Redesigned FL enterprise security by taking the approach of a partner vs an enforcer.
- **Updated Agency Cybersecurity Strategic and Operational Plan (ASOP) process to align to the Statewide Cybersecurity Strategic Plan:**
  - Rebuilt antiquated ASOP process, reduced time agencies had to spend preparing the plan by 75%.
- **Established quarterly Incident Response reporting to map trends in enterprise security**



18

# Building Upon the Success in 2022

## Expanding the Program's Capabilities

- Acquire and deploy a Governance Risk and Compliance software suite
- Provide Identity and Access Management solution(s) for the enterprise
- Provide Multi-factor Authentication solution(s) to the enterprise

## "Whole of State" Cyber to Extend the Reach of the Program Beyond State Government

- \$30m to deploy cybersecurity capabilities to local government entities through a competitive grant program
- Expand cybersecurity training opportunities to state and local entities
- Develop and publish 2023 Statewide Cybersecurity Strategy
- Review and update reporting method for Agency Strategic and Operational Cybersecurity Plans
- Expanding the FIRE Team Footprint to increase incident response times and effectiveness



19

## FL[DS] CSOC - Incident Response Plan

- A **living document**...not intended to be static
- Shaped by government/industry **best practices** and operational **lessons learned**
- Codifies CSOC's **operational** processes and procedures
- Provides a **baseline operations construct** between CSOC and state-wide cybersecurity stakeholders
- Email: [CSOC@digital.fl.gov](mailto:CSOC@digital.fl.gov) for a copy



Florida [Digital Service]

Cybersecurity Operations Center  
Operational Construct & Incident Response Plan

v1.0

2022-2023

\*\* CONFIDENTIAL AND EXEMPT FROM PUBLIC RECORD PURSUANT TO F.S. 119.0725 \*\*



**\*\* CONFIDENTIAL AND EXEMPT FROM PUBLIC RECORD PURSUANT TO F.S. 119.0725 \*\***

20

# House Bill 7057 - Public Records Exemptions

## Aligns local government with state agencies, exempting:

- Coverage limits
- Critical infrastructure information
- Network schematics, hardware and software configurations, and response practices
- Public meetings regarding exempt information

## Additional Requirements

- Reporting ransomware and high severity incident to CSOC
- After action reports
- Adopting cybersecurity standards
- Employee cybersecurity training



21

# Local Government Cybersecurity Grant

	Federal Grant	Florida Plan
Deliverables	Funding & Capabilities*	Capabilities
Match Requirement	Increasing Match Amounts at Local Level	No Match Requirement
Total Amount	\$30 Mil over 4 years	\$30 Mil in FY 22-23
Additional Requirements	Ongoing Monitoring & Recommendations	Cooperation with CSOC

All applications received in response to the federal grant program will be reviewed and all eligible applications will be considered by FL[DS] for participation in the Florida funded grant program.



22

## Local Government Cybersecurity Grant

Governor DeSantis expects Florida to lead the nation in cybersecurity capabilities. That's why he asked for and the legislature responded with \$30m for local government cybersecurity technical assistance grants

### The Florida Plan

- Provide integrated capabilities and avoid complex and bureaucratic grant processes that award money
- No required match funding from the recipient - just partnership
- Maintain your autonomy with Least Privilege Access and DSAs
- Future funding subject to appropriations...

### Functions and Capabilities

- Asset discovery & inventory
- End point detection & response
- Content delivery network
- Incident Response Assistance
- Email security service
- 24/7/365 Monitoring & Response Service



23

## Local Government Cybersecurity Grant

Date	Significance
Early February	Application Published
February 14 <sup>th</sup> - March 31	Application Window
April 1 <sup>st</sup> - April 15 <sup>th</sup>	Scoring
April 15 <sup>th</sup>	Announcement of Initial Grant Awards
TBD	Announcement of Remaining Awards

Program Contact Email: [cybersecuritygrants@digital.fl.gov](mailto:cybersecuritygrants@digital.fl.gov)



24

# Chris Cruz

25

## Tanium Converged Endpoint Management

- Built to ensure great cyber hygiene across Security, Operations and Compliance
- We've been working closely with FLDS to support their efforts across the State Agencies
- We are excited for the opportunity to introduce you to Tanium as a potential tool in your grant application.
- Please reach out so we can support your technology evaluation process and application efforts:  
[adam.r@tanium.com](mailto:adam.r@tanium.com)



26



Questions?