HOUSE OF REPRESENTATIVES
FLORIDA

Energy, Communications & Cybersecurity Subcommittee

Wednesday, October 18, 2023
10:00 AM
Reed Hall (102 HOB)

Meeting Packet

Paul Renner
Speaker

Mike Giallombardo
Chair

The Florida House of Representatives

Commerce Committee

Energy, Communications & Cybersecurity Subcommittee

Paul Renner
Speaker

Mike Giallombardo
Chair

Meeting Packet

Wednesday, October 18, 2023
10:00 am – 11:00 am
Reed Hall (102 HOB)

I. Call to Order

II. Roll Call

III. Welcome and Opening Remarks

IV. Cybersecurity Update from Florida Digital Service

V. Closing Remarks

Cybersecurity | Florida Digital Service

Empowering Florida's Digital Resilience

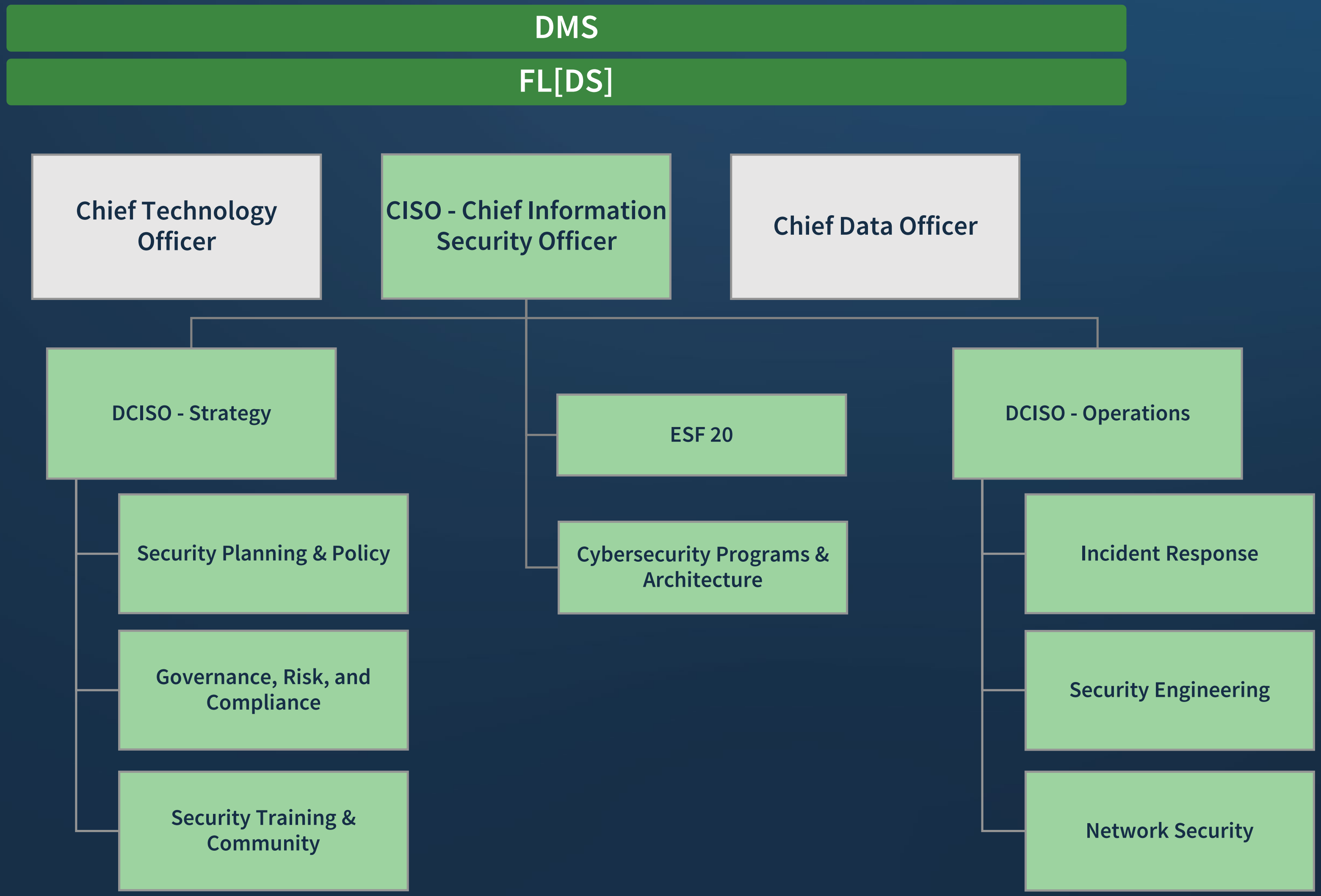
Within the Florida Digital Service, the State Chief Information Security Officer (CISO) is responsible for development, operation, and oversight of cybersecurity for state technology systems.

Our Mission:

- Ensure availability, confidentiality, and integrity of state systems.
- Safeguard state agency digital assets, data, information, and information technology resources.
- Establish standards and processes for assessing state agency cybersecurity risks and determining appropriate security measures.

Delivered through vigilant oversight of the State Cybersecurity Operations Center (CSOC).

Org Chart



DMS

FL[DS]

Chief Technology Officer

CISO - Chief Information Security Officer

Chief Data Officer

DCISO - Strategy

Security Planning & Policy

Governance, Risk, and Compliance

Security Training & Community

ESF 20

Cybersecurity Programs & Architecture

DCISO - Operations

Incident Response

Security Engineering

Network Security

Cybersecurity Requires

Engagement Across the Enterprise

- **Florida Department of Law Enforcement -** Intelligence, investigations, and technical analysis
- **Department of Management Services’ Division of Telecommunications -** Network security and availability
- **Department of State -** Shared resources and support
- **Florida Division of Emergency Management -** Cybersecurity grants and ESF20
- **Many others -** State enterprise agencies, local government entities, universities, etc.

Cyber Community

- FL[DS] CoLab offering ISC2 continuing education credits
  - 22 total cybersecurity sessions
  - 350+ attendees
  - 7 sessions eligible for CEUs since August 2023
- 34 state agencies represented in at least one cybersecurity workgroup
- Enterprise Security Leaders meetings and 6 domain specific workgroups held each month

Cyber Community

Throughout the Month

All agency CSIRTs participating in the *first-ever* enterprise cyber training exercise

October 11

FL[DS] Presents Effective Policy and Processes for Incident Response and Threat Hunting

October 17

FL[DS] Cybersecurity Presents How Traditional Email Defenses Fail Against Modern Attacks

October 20

A Deep Dive into the Local Government Cybersecurity Resource Packet

October 26

Virtual Training Exercise: Anatomy of an Attack

SU	MO	TU	WE	TH	FR	SA
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Cybersecurity Operations Center (CSOC)

Solution Adoption

Enterprise Cybersecurity Solution	Agencies Adopted / Implementing
Cloud-based Unified Security Suite	28
Managed CSOC Solution	24
Asset Discovery (Agent)	17
Asset Discovery (Agentless)	20
External Attack Surface Discovery	34
Endpoint Protection (EDR) / Managed Response Services	24 / 16
Content Delivery Network	13
Licensure and Credential Access Management Platform	8

Security Operations – Extended Response

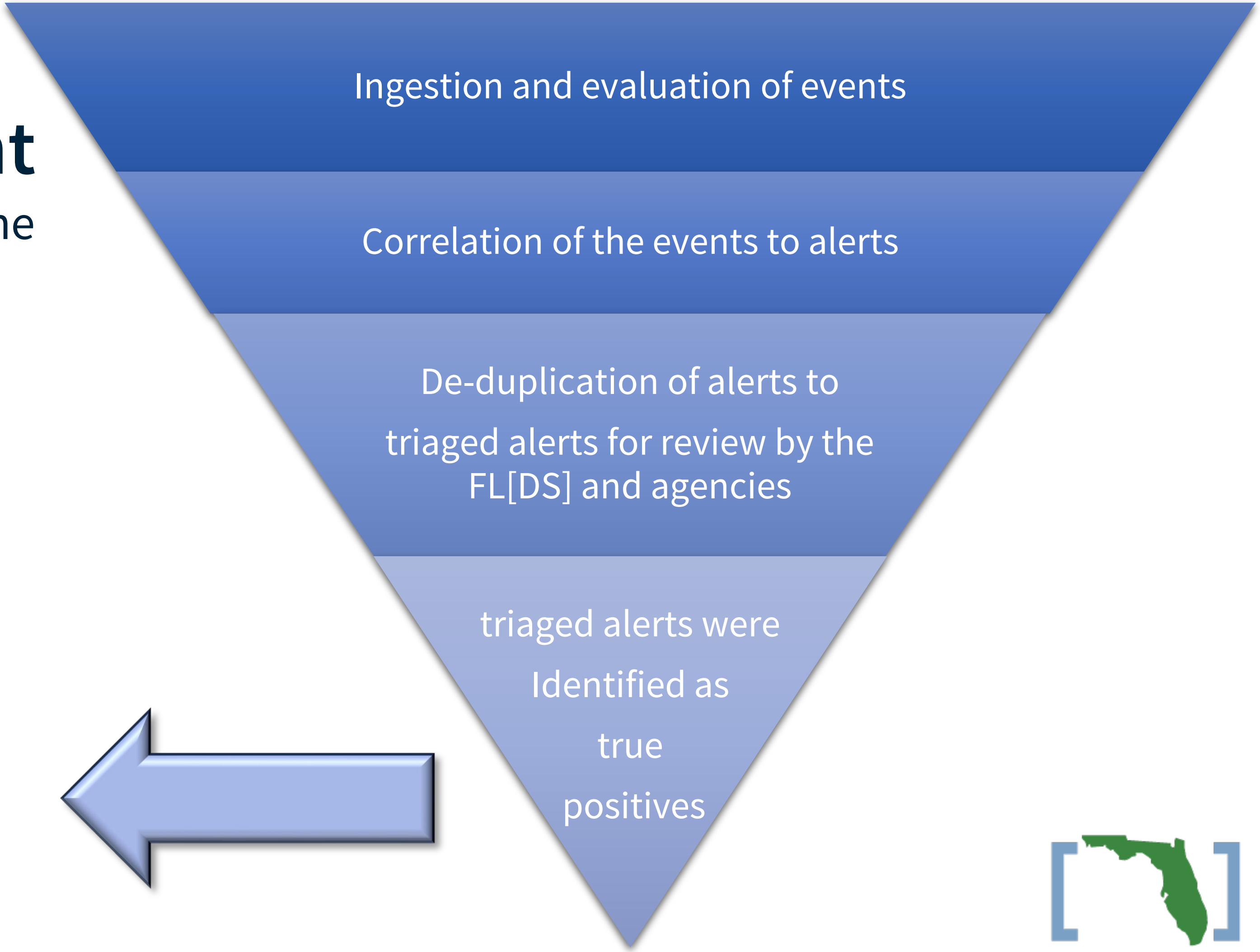
Security Event Management

Significant threat analysis to deal with volume of security event data.

Rapidly correlate against other agencies and share information to prevent other compromises.

Incident Response

Support affected agency efforts to bring an incident under control, expel bad actors, recover their systems.



Ingestion and evaluation of events

Correlation of the events to alerts

De-duplication of alerts to

triaged alerts for review by the FL[DS] and agencies

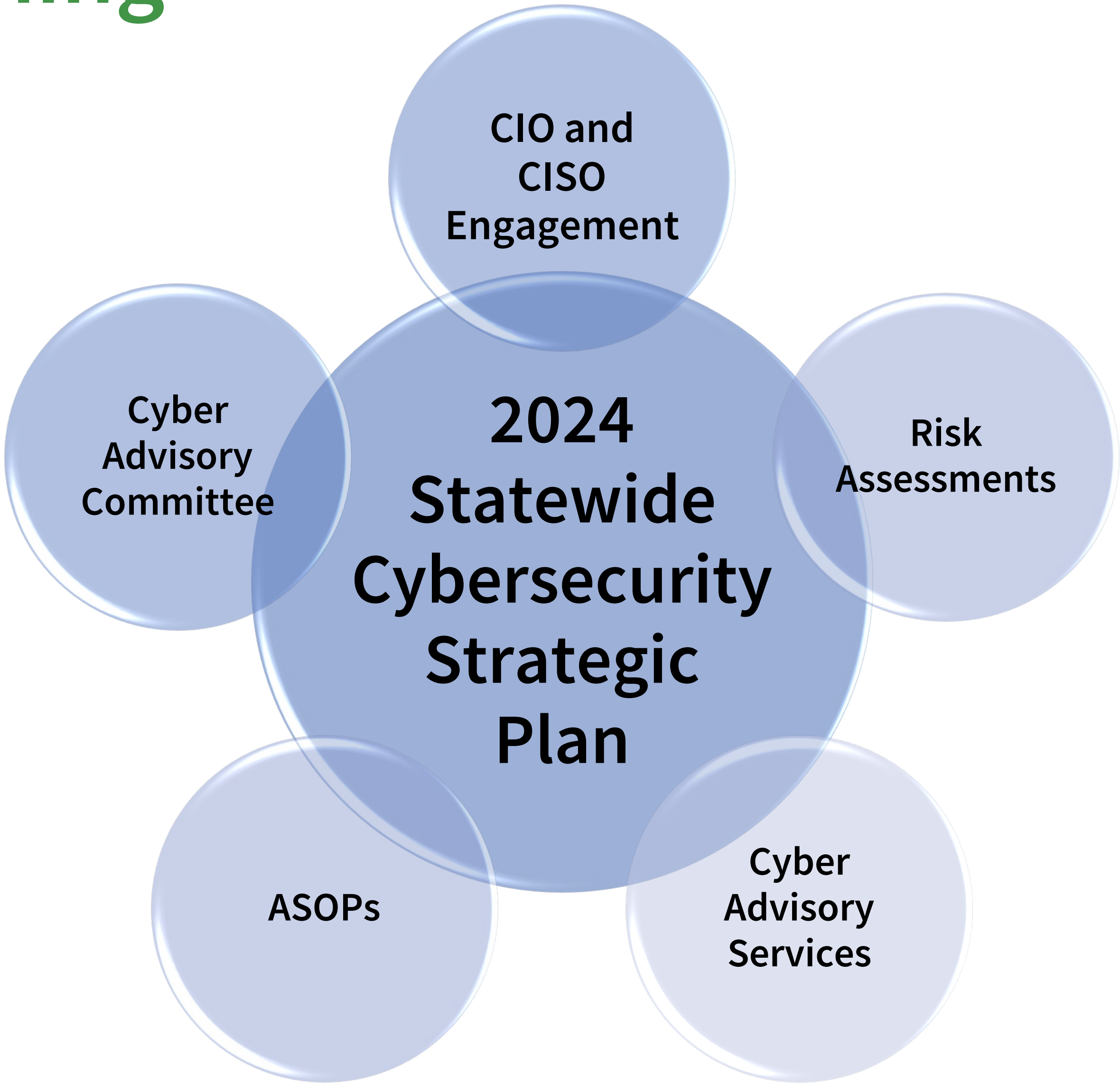
triaged alerts were

Identified as

true

positives

Strategic Planning



2024 Statewide Cybersecurity Strategic Plan

CIO and CISO Engagement

Risk Assessments

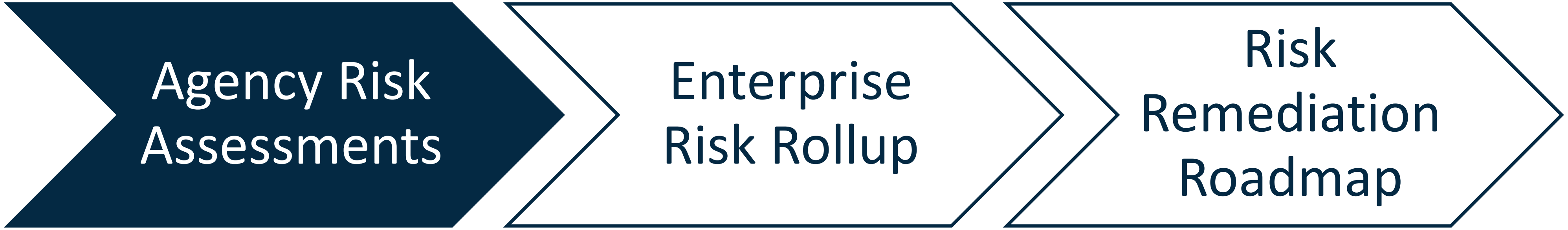
Cyber Advisory Services

ASOPs

Cyber Advisory Committee

Risk & Compliance

Thirty agencies participated in a comprehensive risk assessment.



Agency Risk Assessments

Enterprise Risk Rollup

Risk Remediation Roadmap

Five agencies provided their own results.

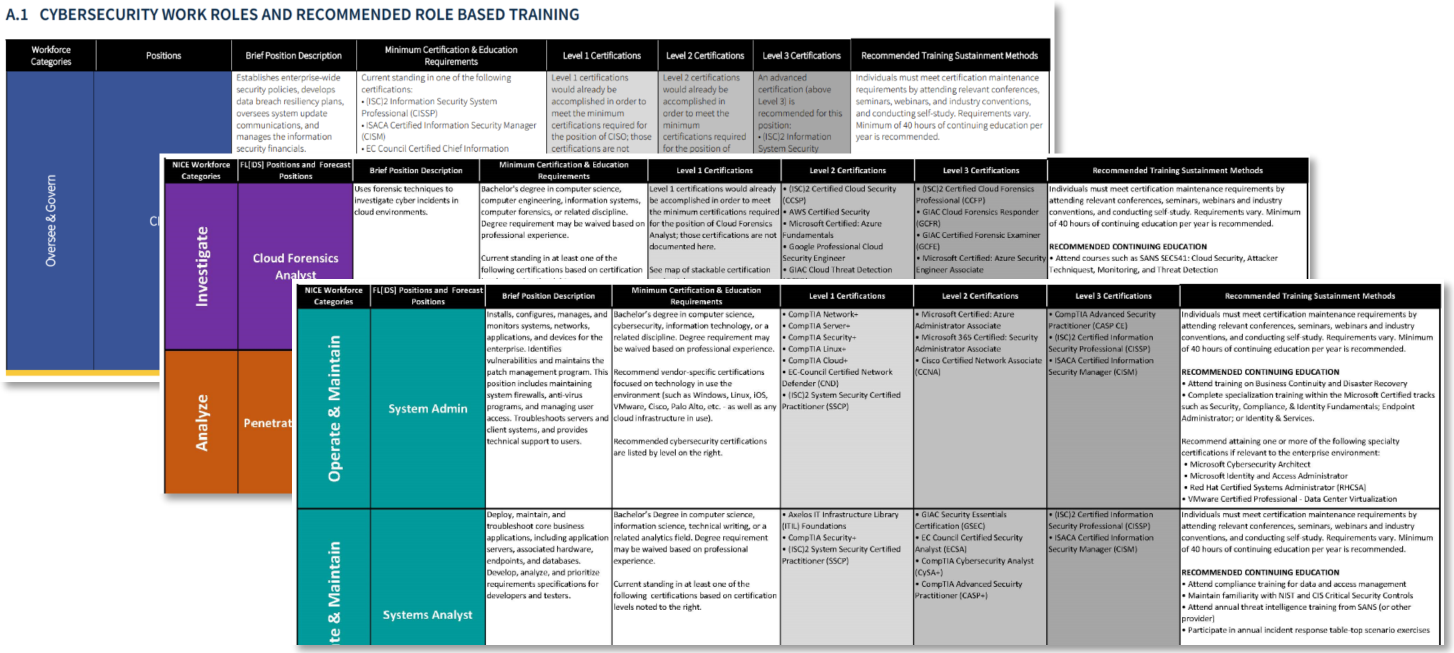
Comprehensive Risk Assessments

Moving forward:

- Gathering requirements for an enterprise Governance, Risk, and Compliance (GRC) platform - **29** agencies indicated demand for a GRC tool in their ASOP.
- 60GG-2 Revisions - Drafting language for the rule. Will use themes uncovered from the risk assessments to incorporate standards.

Cybersecurity Positions and Training Guidelines

- Includes basic descriptions for 36 roles based on NICE framework
- Provides advancement levels and training specifications across 7 domains
- Distributed training curriculum as required by F.S. section 282.3185 & 282.318
  - Security awareness training (all government employees)
  - Advanced cybersecurity training curriculum (for elevated access)



A.1 CYBERSECURITY WORK ROLES AND RECOMMENDED ROLE BASED TRAINING

Workforce Categories	Positions	Brief Position Description	Minimum Certification & Education Requirements	Level 1 Certifications	Level 2 Certifications	Level 3 Certifications	Recommended Training Sustainment Methods
Oversee & Govern	Cl	Establishes enterprise-wide security policies, develops data breach resiliency plans, oversees system update communications, and manages the information security financials.	Current standing in one of the following certifications: • (ISC)2 Information Security System Professional (CISSP) • ISACA Certified Information Security Manager (CISM) • EC Council Certified Chief Information	Level 1 certifications would already be accomplished in order to meet the minimum certifications required for the position of CISO; those certifications are not	Level 2 certifications would already be accomplished in order to meet the minimum certifications required for the position of	An advanced certification (above Level 3) is recommended for this position: • (ISC)2 Information System Security	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars, and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended.

NICE Workforce Categories	FL[DS] Positions and Forecast Positions	Brief Position Description	Minimum Certification & Education Requirements	Level 1 Certifications	Level 2 Certifications	Level 3 Certifications	Recommended Training Sustainment Methods
Investigate	Cloud Forensics Analyst	Uses forensic techniques to investigate cyber incidents in cloud environments.	Bachelor's degree in computer science, computer engineering, information systems, computer forensics, or related discipline. Degree requirement may be waived based on professional experience. Current standing in at least one of the following certifications based on certification	Level 1 certifications would already be accomplished in order to meet the minimum certifications required for the position of Cloud Forensics Analyst; those certifications are not documented here. See map of stackable certification	• (ISC)2 Certified Cloud Security (CCSP) • AWS Certified Security • Microsoft Certified: Azure Fundamentals • Google Professional Cloud Security Engineer • GIAC Cloud Threat Detection	• (ISC)2 Certified Cloud Forensics Professional (CCFP) • GIAC Cloud Forensics Responder (GCFR) • GIAC Certified Forensic Examiner (GCFE) • Microsoft Certified: Azure Security Engineer Associate	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend courses such as SANS SEC541: Cloud Security, Attacker Techniquest, Monitoring, and Threat Detection
Analyze	Penetrat						

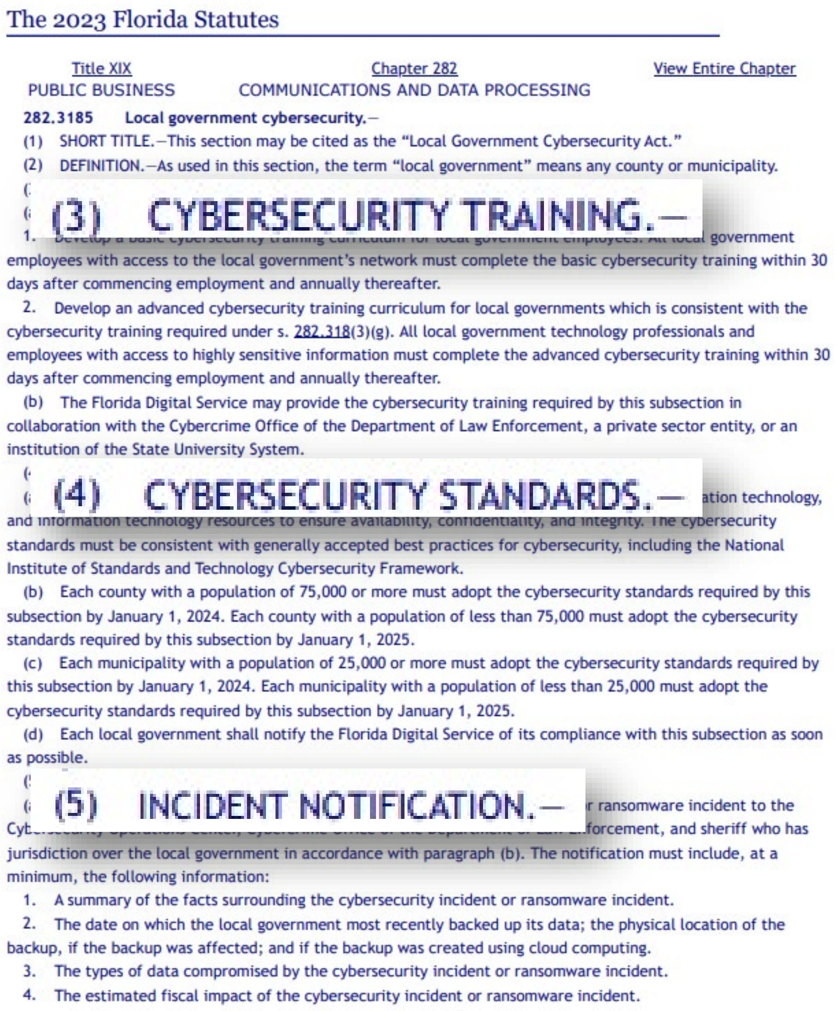
NICE Workforce Categories	FL[DS] Positions and Forecast Positions	Brief Position Description	Minimum Certification & Education Requirements	Level 1 Certifications	Level 2 Certifications	Level 3 Certifications	Recommended Training Sustainment Methods
Operate & Maintain	System Admin	Installs, configures, manages, and monitors systems, networks, applications, and devices for the enterprise. Identifies vulnerabilities and maintains the patch management program. This position includes maintaining system firewalls, anti-virus programs, and managing user access. Troubleshoots servers and client systems, and provides technical support to users.	Bachelor's degree in computer science, cybersecurity, information technology, or a related discipline. Degree requirement may be waived based on professional experience. Recommend vendor-specific certifications focused on technology in use the environment (such as Windows, Linux, iOS, VMware, Cisco, Palo Alto, etc. - as well as any cloud infrastructure in use). Recommended cybersecurity certifications are listed by level on the right.	• CompTIA Network+ • CompTIA Server+ • CompTIA Security+ • CompTIA Linux+ • CompTIA Cloud+ • EC-Council Certified Network Defender (CND) • (ISC)2 System Security Certified Practitioner (SSCP)	• Microsoft Certified: Azure Administrator Associate • Microsoft 365 Certified: Security Administrator Associate • Cisco Certified Network Associate (CCNA)	• CompTIA Advanced Security Practitioner (CASP CE) • (ISC)2 Certified Information Security Professional (CISSP) • ISACA Certified Information Security Manager (CISM)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend training on Business Continuity and Disaster Recovery • Complete specialization training within the Microsoft Certified tracks such as Security, Compliance, & Identity Fundamentals; Endpoint Administrator; or Identity & Services. Recommend attaining one or more of the following specialty certifications if relevant to the enterprise environment: • Microsoft Cybersecurity Architect • Microsoft Identity and Access Administrator • Red Hat Certified Systems Administrator (RHCSA) • VMware Certified Professional - Data Center Virtualization
Operate & Maintain	Systems Analyst	Deploy, maintain, and troubleshoot core business applications, including application servers, associated hardware, endpoints, and databases. Develop, analyze, and prioritize requirements specifications for developers and testers.	Bachelor's Degree in computer science, information science, technical writing, or a related analytics field. Degree requirement may be waived based on professional experience. Current standing in at least one of the following certifications based on certification levels noted to the right.	• Axelos IT Infrastructure Library (ITIL) Foundations • CompTIA Security+ • (ISC)2 System Security Certified Practitioner (SSCP)	• GIAC Security Essentials Certification (GSEC) • EC Council Certified Security Analyst (ECSA) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Secuirty Practitioner (CASP+)	• (ISC)2 Certified Information Security Professional (CISSP) • ISACA Certified Information Security Manager (CISM)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend compliance training for data and access management • Maintain familiarity with NIST and CIS Critical Security Controls • Attend annual threat intelligence training from SANS (or other provider) • Participate in annual incident response table-top scenario exercises

Florida's Inaugural Public Sector Cybersecurity Summit

September 14, 2023

- 375 total attendees
- 275 public sector attendees
- 85 local government attendees
- 21 higher education attendees

Local Government Cybersecurity Packet



The 2023 Florida Statutes

Title XIX PUBLIC BUSINESS | Chapter 282 COMMUNICATIONS AND DATA PROCESSING | View Entire Chapter

282.3185 Local government cybersecurity.—

(1) SHORT TITLE.—This section may be cited as the "Local Government Cybersecurity Act."

(2) DEFINITION.—As used in this section, the term "local government" means any county or municipality.

(3) CYBERSECURITY TRAINING.—

1. Develop a basic cybersecurity training curriculum for local government employees. All local government employees with access to the local government's network must complete the basic cybersecurity training within 30 days after commencing employment and annually thereafter.

2. Develop an advanced cybersecurity training curriculum for local governments which is consistent with the cybersecurity training required under s. 282.318(3)(g). All local government technology professionals and employees with access to highly sensitive information must complete the advanced cybersecurity training within 30 days after commencing employment and annually thereafter.

(b) The Florida Digital Service may provide the cybersecurity training required by this subsection in collaboration with the Cybercrime Office of the Department of Law Enforcement, a private sector entity, or an institution of the State University System.

(4) CYBERSECURITY STANDARDS.—

[illegible] ation technology, and information technology resources to ensure availability, confidentiality, and integrity. The cybersecurity standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework.

(b) Each county with a population of 75,000 or more must adopt the cybersecurity standards required by this subsection by January 1, 2024. Each county with a population of less than 75,000 must adopt the cybersecurity standards required by this subsection by January 1, 2025.

(c) Each municipality with a population of 25,000 or more must adopt the cybersecurity standards required by this subsection by January 1, 2024. Each municipality with a population of less than 25,000 must adopt the cybersecurity standards required by this subsection by January 1, 2025.

(d) Each local government shall notify the Florida Digital Service of its compliance with this subsection as soon as possible.

(5) INCIDENT NOTIFICATION.—

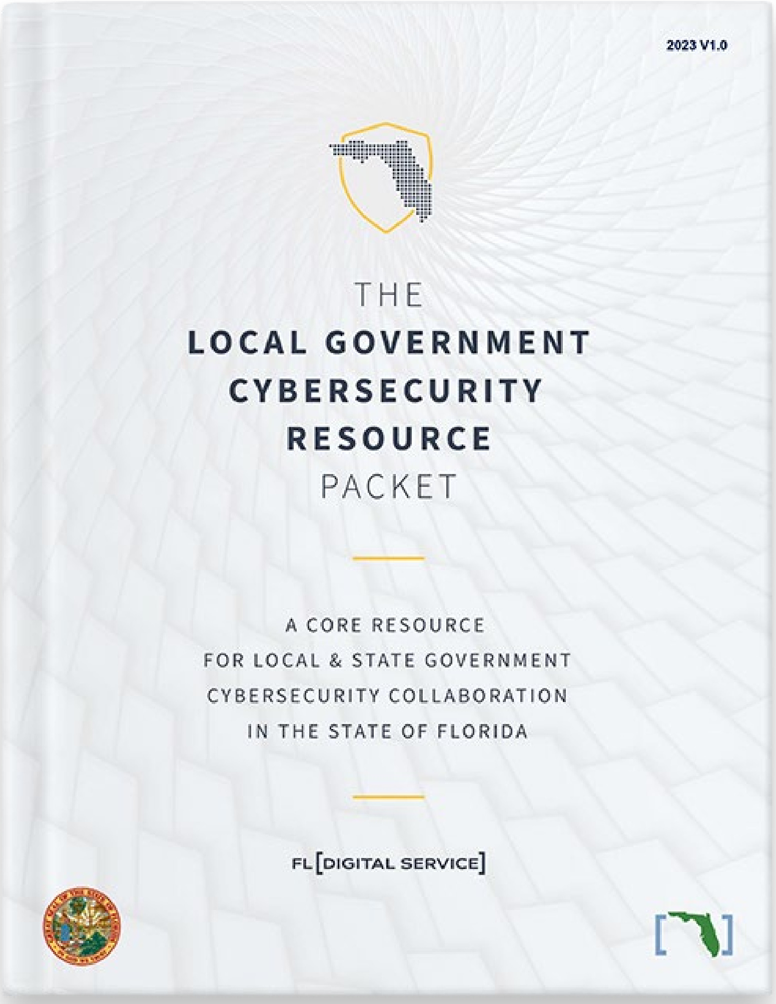
[illegible] r ransomware incident to the Cyb[illegible]forcement, and sheriff who has jurisdiction over the local government in accordance with paragraph (b). The notification must include, at a minimum, the following information:

1. A summary of the facts surrounding the cybersecurity incident or ransomware incident.

2. The date on which the local government most recently backed up its data; the physical location of the backup, if the backup was affected; and if the backup was created using cloud computing.

3. The types of data compromised by the cybersecurity incident or ransomware incident.

4. The estimated fiscal impact of the cybersecurity incident or ransomware incident.



2023 V1.0

THE LOCAL GOVERNMENT CYBERSECURITY RESOURCE PACKET

A CORE RESOURCE FOR LOCAL & STATE GOVERNMENT CYBERSECURITY COLLABORATION IN THE STATE OF FLORIDA

FL[DIGITAL SERVICE]

FY 22-23 Local Grants – Highlights

337 local entities applied for local grants, representing 66 out of Florida’s 67 counties

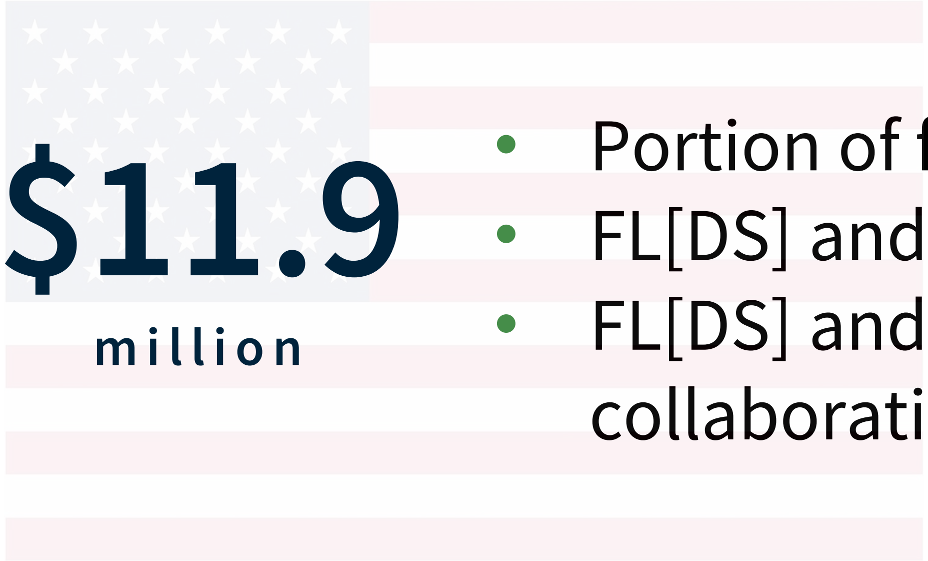
More than 730 deployments of cybersecurity capabilities across 193 local entities

96% of participating local entities committed to sharing cybersecurity data with the CSOC

“It has fulfilled a tremendous need. We are a rural fiscally constrained county and without the assistance we would not have the added security that we have now and hope to continue.”

- Holmes County Sheriff's Office

State & Federal Cybersecurity Grant Programs FY 23-24



$11.9

million

- Portion of funds dedicated to **rural communities**
- FL[DS] and **DEM collaboration** for grant management
- FL[DS] and **Domestic Security Oversight Council** (DSOC) collaboration for planning committee

$40

million

- Focused on Florida local governments
- Funding for cybersecurity **risk management** programs
- Emphasis on risk management programs, cybersecurity standards, and **vulnerability mitigation**

Questions?

Please contact Jeff Ivey, Deputy Chief of Staff

Jeff.Ivey@dms.fl.gov