2023 V1.1

THE LOCAL GOVERNMENT CYBERSECURITY RESOURCE PACKET

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

FL[DIGITAL SERVICE]

Table of Contents

Introduction

The Local Government Cybersecurity Resource Packet is a collection of essential materials and guidelines designed to support local governments in complying with the various administrative rules and statutes that address the security of state and local information systems. This packet serves as a valuable reference guide, offering practical information, best practices, and tools to enhance the security posture of the local governments in Florida.

digital.fl.gov/cyber

A Word From State Chief Information Security Officer (CISO) Jeremy Rodgers

Local Partners & Colleagues,

It is our job to help secure the information of over 22 million Floridians. Here at the Florida Digital Service, we take this responsibility seriously, and we are committed to striving towards reaching the highest levels of security to ensure the confidentiality, integrity, and availability of all data. We know that we cannot do this alone, and we appreciate the hard work and dedication that you bring to this critical mission.

Having previously served in local government, I'm acutely aware that your primary responsibility is to your constituents and that challenges can vary significantly from one municipality or city to another. I also recognize that trust between partners is hard-earned but easily lost. Your partnership is crucial to the success of our collective efforts. We are deeply grateful for your expertise, resources, and steadfast support.

On behalf of our entire team, I want to express our sincere thanks for all that you do for our great state. Your contributions are truly valued, and we look forward to continuing our partnership as we work together to protect the privacy and security of our citizens.

Very Respectfully,

Jeremy Rodgers

Section 1: Information Security Program

Overview of Information Security Management

The National Institute of Standards and Technology's (NIST) approach to information security management, as outlined in Special Publication 800-53 Revision 5, involves the following key steps:

Risk Assessment: Identifying threats, vulnerabilities, and impacts to information systems.

Security Controls: Implementing a catalog of security control to protect systems.

Security Categorization: Categorizing systems based on their potential impact.

Security Assessment: Regularly evaluating the effectiveness of security controls.

Continuous Monitoring: Monitoring and analyzing security-related events and system performance.

Incident Response: Developing and implementing plans to respond to security incidents.

Security Awareness and Training: Educating employees about their security roles and responsibilities.

Security Authorization: Documenting and obtaining management approval for security plans.

Importance of Information Security

As emphasized by the National Institute of Standards and Technology (NIST), robust information security measures are essential to protect the confidentiality, integrity, and availability of sensitive data and critical systems. By safeguarding information against unauthorized access, modification, or disclosure, organizations can maintain trust and confidence among their stakeholders. A comprehensive approach to information security ensures the resilience and continuity of operations, bolstering the overall stability and competitiveness of organizations in an increasingly interconnected and digital world.

Roles and Responsibilities

Below is a list of common cybersecurity roles which are responsible for the performance of cybersecurity programs and the defense of state and local assets from threat actors.

State of Florida State CISO (Chief Information Security Officer):

- **Identify:** Oversees the establishment of a cybersecurity strategy for the entire state, ensuring that it aligns with state and federal regulations.
- **Protect:** Develops, implements, and manages the state's overall cybersecurity policies.
- **Detect:** Sets up the state Cybersecurity Operations Center and oversees monitoring and intelligence.
- **Respond:** Acts as the focal point during statewide cybersecurity incidents.
- **Recover:** Orchestrates recovery operations after a cybersecurity incident.

State of Florida Chief Inspector General

- **Identify:** Conducts or oversees audits and investigations to identify vulnerabilities, inefficiencies, and non-compliance with state and federal laws related to cybersecurity.
- **Protect:** Reviews the effectiveness of security controls and protective measures implemented by state agencies, recommending improvements where necessary.
- **Detect:** Evaluates the state agencies' ability to detect cybersecurity incidents in a timely and effective manner, ensuring that monitoring and alerting systems are operational and effective.
- **Respond:** Audits and reviews incident response plans and actual responses to cybersecurity incidents, ensuring they align with state and federal regulations.
- **Recover:** Reviews post-incident recovery activities to ensure that they follow best practices and guidelines, ensuring lessons are learned and future vulnerabilities are addressed.

State and Local Chief Information Security Officers

- **Identify:** Works with the State CISO to develop and tailor cybersecurity policies for their respective agencies.
- **Protect:** Implements security measures to safeguard the agency's digital assets.
- **Detect:** Monitors agency-specific threats and vulnerabilities.
- **Respond:** Manages agency-specific incidents, coordinating with the State CISO.
- **Recover:** Develops and implements recovery plans at the agency level.

State and Local Information Security Managers

- **Identify:** Assists the CISO in identifying the assets and risks pertaining to their agency.
- **Protect:** Helps implement security protocols based on policy directives from the CISO.

- **Detect:** Supervises the daily security operations and threat detection mechanisms.
- **Respond:** Acts as a first responder within the agency for any cybersecurity incidents.
- **Recover:** Helps restore and validate system functionality for business operations after an event.

State and Local Inspector Generals

- **Identify:** Audits current systems to identify vulnerabilities or compliance issues.
- **Protect:** Recommends protective measures based on audit findings.
- **Detect:** May not be directly involved but would review incident detection capabilities during audits.
- **Respond:** Reviews incident response strategies and procedures to ensure effectiveness.
- **Recover:** Evaluates the effectiveness of recovery plans and activities post-incident.

State and Local Incident Response Teams

- **Identify:** Not directly involved but may provide input based on lessons learned from past incidents.
- **Protect:** Implements protective measures during an incident to prevent further damage.
- **Detect:** Constantly monitors for signs of incidents and verifies them.
- **Respond:** Takes immediate action to contain and mitigate incidents.
- **Recover:** Assists in recovery activities to restore and validate system functionality.

State and Local Security Architects, Engineers, and Analysts

- **Identify:** Evaluates system architecture for vulnerabilities; engineers focus on building secure systems, and analysts identify threats.
- **Protect:** Architects and engineers implement security controls; analysts recommend protective measures.
- **Detect:** Analysts actively monitor security alerts, while architects and engineers ensure systems are built for effective monitoring.
- **Respond:** Analysts provide initial assessments and necessary information to respond to incidents. Engineers may assist in containment activities.
- **Recover:** Engineers and architects focus on rebuilding a secure system; analysts might focus on lessons learned.

Contact Information

General Cybersecurity: Security@digital.fl.gov

This email address serves as the primary point of contact for all cybersecurity-related matters. Whether it's questions about security policies or inquiries about cybersecurity initiatives, this inbox is monitored by a team responsible for ensuring the digital safety of state services and data.

Incident Response: CSOC@digital.fl.gov or http://IR.digital.fl.gov (website)

This email is a dedicated channel for reporting and managing cybersecurity incidents. If there's a security breach, suspected phishing attempt, or other types of cyber incidents, this is the immediate point of contact. It's monitored 24/7 by a specialized Incident Response Team that springs into action to manage and mitigate any reported incidents.

Office of Data Management: Data@digital.fl.gov

This is the contact for questions, concerns, or issues related to data management. This includes queries about data governance, data quality, data privacy, and compliance with data-related regulations. The team managing this inbox is skilled in ensuring the quality and integrity of data across state systems.

Customer Experience: Service@digital.fl.gov

This email is dedicated to questions about project management, oversight, principles, standards, and best practices as well as information about current or upcoming technology project managed by FL[DS]. This inbox is managed by a team of customer service professionals who can provide updates, relay your suggestions, or route your inquiry to the appropriate project lead to assist you.

Office of the State Chief Information Officer: CIO@digital.fl.gov

This is the dedicated inbox for the office of the State CIO. If your inquiry requires executive level attention, this is the place to send it.

FL[DS] CoLab Events: CoLab@digital.fl.gov

The FL[DS] CoLab is a sales-free, collaborative environment dedicated to offering enterprise team members a full slate of on-going technology training, awareness, and professional development opportunities. Use this dedicated inbox to learn about upcoming events, be added to the mailing list or schedule a meeting to discuss presenting in the CoLab.

Section 2: Cybersecurity Training

2.1 Training Requirements

Florida Statutes section 282.3185(3) - Local government cybersecurity, Cybersecurity Training:

Basic Cybersecurity Training (awareness)

The Florida Digital Service shall 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.

Advanced Cybersecurity Training (role-based)

The Florida Digital Service shall develop an advanced cybersecurity training curriculum for local governments which is consistent with the cybersecurity training required under s. 282.318(3)(g).

http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0200-0299/0282/Sections/0282.318.html

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.

2.2 Cybersecurity Awareness and Training

Cybersecurity awareness and training are essential components of protecting individuals and organizations from cyber threats.

Cybersecurity Awareness

A cybersecurity awareness campaign is a focused initiative designed to increase awareness about cybersecurity best practices to the general population. Cybersecurity awareness is considered a passive activity primarily achieved through posters, billboards, flyers, newsletters, and broadcast advertisements. The purpose of awareness is to focus attention on best practices for physical security, avoiding online scams, and social engineering. Cybersecurity awareness is the first building block in developing a cybersecurity awareness and training program.

Recommendations

Provide visual reminders such as posters, flyers, and newsletters to reinforce training and education and help to promote a cybersecurity-conscious culture.

Establish centralized coordination of providing cybersecurity awareness materials and guidelines to agencies.

Cybersecurity Awareness Training

EMPLOYEES WITH NETWORK ACCESS: Reinforcing cybersecurity concepts in multiple formats allows individuals to recognize cyber threats and consider changing behavior. Training builds upon the cybersecurity awareness campaign by providing a more intentional and interactive experience. For all employees, it is important to keep cybersecurity threats and cyber hygiene best practices top of mind. Cybersecurity awareness training should include acknowledgement of policies and procedures within the organization at onboarding and again annually as organizational guidance changes.

Curriculum

Introduction to Cybersecurity Awareness

- Importance of cybersecurity for individuals and organizations
- Basic terminology and concepts in cybersecurity
- Role and responsibility of users in network security

Recognizing Common Cyber Threats

- Phishing attacks and email scams
- Malware (viruses, ransomware) and its impact
- Social engineering techniques (e.g., impersonation, pretexting)

Password Security and Authentication

- Importance of strong, unique passwords
- Best practices for creating and managing passwords

Safe Web Browsing and Email Practices

- Identifying malicious websites and links
- Secure web browsing habits (HTTPS, avoiding unknown downloads)
- Email security practices (suspicious attachments, email hygiene)

Secure Mobile Device Usage

- Mobile security threats and vulnerabilities
- Safe app installation and updates
- Protecting mobile devices (screen locks, remote wipe)

Social Media and Online Privacy

- Privacy settings and permissions on social media platforms
- Risks of oversharing personal information
- Safeguarding online reputation and privacy

Network Security Best Practices

- Safe usage of public Wi-Fi networks
- Secure home network configurations (router settings, encryption)
- Understanding and using firewalls

Data Protection and Backup Strategies

- Importance of data backup and disaster recovery
- Cloud storage security considerations
- Encrypting sensitive data and files

Incident Reporting and Response

- Recognizing and reporting security incidents
- Steps to take in case of a suspected breach or attack.
- Role of users in incident response and cooperating with IT teams

Ongoing Cybersecurity Awareness

- Staying updated on latest threats and security news.
- Continued education and professional development opportunities
- Promoting a culture of cybersecurity within the organization

2.3 Cybersecurity Role-Based Training

Role-based cybersecurity training expands awareness training to address the specific needs for positions within IT infrastructure, cybersecurity operations, incident response, and cybersecurity management.

EXECUTIVES & MANAGERS: Executives & Managers is a target audience group who may not have direct cybersecurity responsibilities, but they must understand the cybersecurity risks inherent in their positions. Given their access to confidential data and their capacity to make crucial decisions, executives and managers frequently find themselves in the crosshairs of cyber attackers. Additionally, their role in shaping the cybersecurity culture within their departments significantly affects the conduct and awareness of their teams when it comes to cybersecurity.

Recommendations

Tailoring cybersecurity awareness training would be beneficial. The selection and coordination of training topics should include the following:

- Cybersecurity fundamentals
- Risk management
- Security governance and policies
- Security awareness and threat awareness
- Incident response and crisis management including disaster recovery and continuity of operations (COOP)
- Vendor management and Third-Party Risk Management (TPRM)
- Cyber risks of emerging technology and trends

SYSTEM DEVELOPERS & IT PERSONNEL: The System Developers & IT Personnel target audience group was developed to emphasize the additional security concerns involved with infrastructure design and support, network services, and system administration.

Recommendations

System Developers & IT Personnel must be trained in cybersecurity best practices focused within their disciplines such as secure coding for application developers, zero-trust for

system architects and engineers, and vulnerability assessment for system administrators. Formal education courses should be focused on the hands-on activities mapped within recommended professional cybersecurity certifications.

- Support baseline certification tracks within specific work roles as outlined in Appendix A.
- Provide individual training through relevant on-demand labs. Training should be focused on the toolsets and simulated infrastructure of the enterprise environment.
- Develop Job Qualifications Requirements (JQRs) for individuals to prove skills and abilities necessary for the position and for supervisors to monitor resource progression.

CYBERSECURITY SPECIALIST PERSONNEL: The Cybersecurity Specialist Personnel target audience require dedicated hands-on training.

Recommendations

Although incident response training is essential to help ingrain practices and procedures, identify gaps and weaknesses, and promote collaboration, it should only be considered one area of skill development training for a cybersecurity workforce. Multiples categories of expertise are necessary to create a well-functioning CSOC and incident response team.

The crawl, walk, run approach to training a cybersecurity workforce begins with individual education and training which may be achieved through formal education and professional certifications. See Appendix A for detailed cybersecurity baselines to build the foundation for individual positions. This foundation must be enhanced by hands-on cyber lab challenges which follow internal policies and focus on the enterprise tools in use. Individuals also need team training to promote collaboration, to cross-pollinate skills, and to provide opportunities to test the security of the enterprise.

SENIOR CYBERSECURITY MANAGEMENT: Senior cybersecurity managers are in a unique position of having to know everything about the security of the enterprise within which they operate including people, processes, and policies surrounding the technology in use. Multiple topics should be covered in-depth and could be achieved through conference attendance or presentations, re-certification or training classes, or formal education.

Recommendations

Continuous education and training will help senior cybersecurity managers understand the evolving cybersecurity landscape. These leaders need to stay informed about the latest cybersecurity emerging threats and trends as well as regulations and compliance

frameworks including data privacy, risk management, and governance. Leaders must learn to manage third-party risk such as vendor and supply-chain risk management, and have training in cybersecurity strategy development, budgeting, resource management, and team building. A senior cybersecurity manager must represent a strong culture of cybersecurity, and this can be done by learning about employee training methodologies and behavior change techniques.

Additionally, as cloud technologies continue to play a significant role in IT infrastructures, managers should learn about cloud architecture, cloud-specific security controls, and cloud provider management including contract issues such as lock-in. On a more technical level, senior cybersecurity managers may find it beneficial to gain a deeper understanding of offensive security techniques through ethical hacking and penetration testing courses. As a leader of a cybersecurity department or division, the manager must maintain an understanding of current cybersecurity threats as well as the tactics, techniques, and procedures (TTPs) of adversaries. Attending MITRE ATT&CK training and participating in incident response exercises will help in leading incident response teams and managing recovery efforts.

CYBERSECURITY INCIDENT REPONSE TEAM (CSIRT): To provide comprehensive Incident Response, the CSIRT should include members of the Cybersecurity Specialist target audience whose responsibility is to monitor systems, identify and contain incidents, and conduct forensic investigations. Members of the System Development & IT Personnel target audience should be included to assist in isolating networks and systems and to implement technical controls.

Additionally, non-technical members such as legal and compliance, communications and public relations, and human resources may be necessary to manage the business impacts of a cybersecurity incident. Executive management will need to be involved in oversight, direction, and allocating resources. Department managers from individual business units need to provide insight into the potential impact of the incident on their respective areas. And lastly, external partners may need to be included for incident response services, law enforcement follow up, legal counsel, or regulatory authority guidance.

Recommendations

Once established, training for the CSIRTs should be conducted at least annually and in-person. Updates to incident response plans or capabilities should be communicated throughout the year. In addition to incident response training, these teams should be familiar with disaster recovery and continuity of operations plans. Working sessions to create and update the incident response plan (IRP), disaster recovery plan (DRP), and a continuity of

operations plan (COOP) should be prioritized before conducting an incident response table-top exercise. Everyone involved in the CSIRT must be aware of the policies and procedures developed in these plans before being expected to respond to an incident.

2.4 Training Resources

Florida Center for Cybersecurity at University of South Florida

The CyberSecureFlorida training initiative is authorized by Florida Legislation HB5001, Section 2944B, directing the Center to conduct specialized cybersecurity training for various sectors of public employment.

Eligibility: Free to any Florida-based public sector employee, including but not limited to, state, county, and municipal employees, elected officials, law enforcement personnel, public school teachers, and public college and university employees.

GENERAL STAFF: Self-paced online courses covering cybersecurity awareness topics such as phishing and business email compromise.

EXECUTIVE & MANAGERIAL: Courses of various lengths, covering cyber risk management, incident response, and business continuity planning.

TECHNICAL: Training ranging from one to eight weeks that prepare technical personnel for industry certifications, with exam vouchers included.

Links for more information and courses through Florida Center for Cybersecurity:

https://usfcorporatetraining.catalog.instructure.com/browse/cyber/courses/cyber

https://gordoninstitute.fiu.edu/cybersecurity-policy/cybersecureflorida/index.html

https://uwf.edu/centers/center-for-cybersecurity/workforce-development/uwf-florida-cybersecurity-training-program/

FL[DS] CoLab Events:

The FL[DS] CoLab is a sales-free, collaborative environment dedicated to offering enterprise team members a full slate of on-going technology training, awareness, and professional development opportunities. The ever-evolving calendar of events also includes interactive training in the mission critical areas of leadership, project management, cybersecurity, procurement, policy, compliance, cloud modernization, and more. Events also odder an opportunity for individuals to meet, collaborate, and discuss ongoing topics and initiatives important to their organizations. This networking opportunity helps to develop standards and communities of practice among professionals. Please note:

- International Informational System Security Certification Consortium (ISC2) Continuing Professional Education (CPE): Select CoLab events qualify for CPE credits toward maintaining credentials.
- Project Management Professional (PMP) Professional Development Unit (PDU): Select events qualify for PDUs toward maintaining credentials.
- Event Formant: CoLab events are in person and designed to provide an immersive, interactive experience.
- Notification: To receive updates on upcoming FL[DS] CoLab events and to find out which sessions qualify for ISC2 CPEs or PMP Continuing Education, or for more information about CoLab, CoLab@digital.fl.gov.

Other Free Training Opportunities:

ISC2's FREE Certified in Cybersecurity (CC) Training

ISC2 offers free online, self-paced Certified in Cybersecurity (CC) training and exams to one million people. The course is designed to help participants understand the foundational aspects of cybersecurity.

https://www.isc2.org/landing/1mcc

CISA's General Public Training

The Cybersecurity and Infrastructure Security Agency (CISA) offers various cybersecurity training exercises designed for the general public.

https://www.cisa.gov/cybersecurity-training-exercises

SANS Free Training

SANS Institute offers the Cyber Aces Online Courses, which are free and focus on the fundamentals of cybersecurity.

https://www.sans.org/cyberaces/

For any additional questions or recommendations for inclusion in our training resource packet, please contact us.

Section 3: Cybersecurity Standards

3.1 Requirements

Florida Statutes section 282.3185(4) - Local government cybersecurity, Cybersecurity Standards:

a) Each local government shall adopt cybersecurity standards that safeguard its data, information 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.

3.2 Risk Management

Risk management is the ongoing process of identifying, assessing, and responding to risk. The Framework for Improving Critical Infrastructure Cybersecurity (also known as the NIST Cybersecurity Framework or CSF) is a key tool for cybersecurity risk management including the identification, assessment, and maintenance of cybersecurity risk. The NIST CSF is based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders. By using the NIST CSF, organizations can determine activities that are important to critical service delivery, helping to prioritize their investments.

To manage cybersecurity risks, a clear understanding of the organization's business drivers and security considerations specific to its use of technology is required. With each organization's risks, priorities, and systems being unique, the tools and methods used to achieve the outcomes described by the NIST CSF will vary. Source: https://www.nist.gov/cyberframework

The NIST CSF website provides resources for implementing the NIST CSF including a crosswalk to other frameworks such as NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*.

Additional resource:

https://csf.tools/reference/nist-cybersecurity-framework/v1-1/

3.2 Cybersecurity Standards Overview

Pursuant to section 282.3185(4)(a), Florida Statutes, each local government shall adopt cybersecurity standards that safeguard its data, information 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 (NIST) Cybersecurity Framework.

There are multiple national standards and frameworks that can be used to develop standards and implement security programs within your organization. In this handbook, we will be focusing on the NIST CSF Framework. It is a flexible and risk-based approach to managing and improving cybersecurity within organizations. Here is a high-level overview of the framework's key components:

Core Functions: The CSF is built upon five core functions that provide a systematic approach to managing cybersecurity risks:

Identify: Understand and manage cyber risks to systems, assets, data, and capabilities.

Protect: Implement safeguards to prevent or limit the impact of cybersecurity incidents.

Detect: Develop and implement capabilities to identify cybersecurity events promptly.

Respond: Take appropriate actions to mitigate the impact of cybersecurity incidents.

Recover: Restore affected systems, services, and capabilities to normal operations after a cybersecurity incident.

Implementation Tiers: Define four implementation tiers that reflect the maturity and sophistication of an organization's cybersecurity risk management process. Tiers range from Partial (Tier 1) to Adaptive (Tier 4), with increasing levels of integration and effectiveness.

Framework Core: The framework core consists of five functional categories that provide detailed guidance for implementing the core functions. These categories are further divided into subcategories that focus on specific outcomes, activities, and desired results.

Profile: An organization can create a cybersecurity profile by aligning its current cybersecurity activities with the desired outcomes outlined in the framework. The profile helps organizations prioritize and assess their program towards cybersecurity goals.

Informative References: The CSF provides informative references, such as industry standards, best practices, and guidelines, that organizations can use to support the implementation of the framework.

3.2 Compliance Reporting

Florida Statute 282.3185 states each local government shall notify the Florida Digital Service of its compliance with this subsection as soon as possible.

Visit digital.fl.gov/localgovernment-attestation-form to submit an online attestation, affirming your compliance. This attestation should cover:

- Your local government's recognition of the requirement.
- The standard adopted by your local government.
- The contact details of your local government's cybersecurity representative.

Section 4: Cybersecurity Incident Response

4.1 Requirements for Incident Notification

Florida Statutes section 282.3185(5) - Local government cybersecurity, Incident Notification:

(a) A local government shall provide notification of a cybersecurity incident or ransomware incident to the Cybersecurity Operations Center, Cybercrime Office of the Department of Law Enforcement, and sheriff who has jurisdiction over the local government.

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.
5. In the case of a ransomware incident, the details of the ransom demanded.
6. A statement requesting or declining assistance from the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, or the sheriff who has jurisdiction over the local government.

(b) 1. A local government shall report all ransomware incidents and any cybersecurity incident determined by the local government to be of severity level 3, 4, or 5 as provided in s. 282.318(3)(c) to the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government as soon as possible but no later than 48 hours after discovery of the cybersecurity incident and no later than 12 hours after discovery of the ransomware incident. The report must contain the information required in paragraph (a).

2. The Cybersecurity Operations Center shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incident as soon as possible but no later than 12 hours after receiving a local government's incident report. The notification must include a high-level description of the incident and the likely effects.

(c) A local government may report a cybersecurity incident determined by the local government to be of severity level 1 or 2 as provided in s. 282.318(3)(c) to the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government. The report shall contain the information required in paragraph (a).

(d) The Cybersecurity Operations Center shall provide a consolidated incident report on a quarterly basis to the President of the Senate, the Speaker of the House of Representatives, and the Florida Cybersecurity Advisory Council. The report provided to the Florida Cybersecurity Advisory Council may not contain the name of any local government, network information, or system identifying information but must contain sufficient relevant information to allow the Florida Cybersecurity Advisory Council to fulfill its responsibilities as required in s. 282.319(9).

(6) AFTER-ACTION REPORT. —A local government must submit to the Florida Digital Service, within 1 week after the remediation of a cybersecurity incident or ransomware incident, an after-action report that summarizes the incident, the incident's resolution, and any insights gained as a result of the incident.

The incident response process begins with the declaration of a confirmed or suspected incident or threat. In this context, "declaration" refers to the identification of an incident and how to effectively communicate/coordinate Incident Response (IR) information to the CSOC.

History.—s. 3, ch. 2022-220.

4.2 Cybersecurity Incident Response Team

A cybersecurity incident response team (CIRT) is a dedicated group of professionals within the organization responsible for managing and responding to cybersecurity incidents. The primary purpose of the CIRT is to minimize the impact of security incidents, protect the agency's systems and data, and ensure a swift and effective recovery from cyber threats.

It is recommended that CIRT members convene immediately, upon notice of Cybersecurity Incidents. Best practices recommend the responsibilities of CIRT members include:

1. Convening a simple majority of CIRT members at least quarterly to review, at a minimum, established processes and escalation protocols.
2. Receiving incident response training annually.
3. The CIRT shall determine the appropriate response required for each Cybersecurity Incident.

Communications

It is recommended that each organization coordinate response activities with internal and external Stakeholders, as appropriate. Each organization may:

(a) Inform Workers of their roles and order of operations when a response is needed.

(b) Require that Incidents be reported consistent with established criteria and in accordance with Incident reporting procedures. Criteria shall require immediate reporting, including instances of lost identification and Authentication resources.

(c) Share information, consistent with response plans.

(d) Coordinate with Stakeholders, consistent with response plans.

(e) Establish communications with external Stakeholders to share and receive information to achieve broader cybersecurity situational awareness. Where technology permits, enable automated security alerts. Establish processes to receive, assess, and act upon security advisories.

Analysis

It is recommended that each organization conduct analysis to adequately respond and support recovery activities. Related activities may include:

(a) Each organization may establish notification thresholds and investigate notifications from detection systems.

(b) Each organization may assess and identify the impact of Incidents.

(c) Each organization may perform forensics, where deemed appropriate.

(d) Each organization may categorize incidents, consistent with response plans. Each Incident report and analysis, including findings and corrective actions, may be documented.

(e) Establish processes to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources.

Mitigation

It is recommended that each organization perform Incident mitigation activities. The objective of Incident mitigation activities shall be to attempt to contain and prevent recurrence of Incidents; mitigate Incident effects and resolve the Incident; and address vulnerabilities or document as accepted risks.

Improvements

It is recommended that each organization improve organizational response activities by incorporating lessons learned from current and previous detection/response activities into response plans.

Local Government Incident Reporting Process

Three Ways to Contact Us

IR.Digital.FL.gov – preferred method for Incident Reporting

CSOC@Digital.FL.gov

CSOC Phone: (850) 412-6074

IR.digital.fl.gov

Reporting to Law Enforcement

- The FL[DS] Cybersecurity Operations Center (CSOC) reports all incidents to FDLE.
- The CSOC will work with your organization and FDLE to coordinate notification to local law enforcement.

Incident Severity Levels:

- Level 5 is an emergency-level incident that poses an imminent threat to life, wide-scale critical infrastructure, or national, state, or local government security.
- Level 4 is a severe-level incident likely to result in significant impact to public health, safety, liberty, economic security or public confidence.
- Level 3 is a high-level incident likely to result in demonstrable impact to public health, safety, liberty, economic security or public confidence.
- Level 2 is a medium-level incident that may impact to public health, safety, liberty, economic security or public confidence.
- Level 1 is a low-level incident that is unlikely to impact to public health, safety, liberty, economic security or public confidence.

Timeframes, Breach Reporting and Assistance:

- Report all ransomware incidents and any level 3, 4, or 5 cybersecurity incidents as soon as possible but no later than 48 hours after discovery of the cybersecurity incident and no later than 12 hours after discovery of the ransomware incident.
- Local governments can request IR assistance, and FL[DS] will strive to provide support.
- Any security breach affecting 500 or more individuals in Florida must be provided to the Department of Legal Affairs within 30 days as prescribed in F.S. 501.171(3).

Section A: Appendix

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	CISO	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 Security Officer (CCISO) Preferred qualification: Bachelor's degree in information technology, cybersecurity, computer science or other related discipline.	Level 1 certifications would already be accomplished in order to meet the minimum certifications required for the position of CISO; those certifications are not documented here. See map of stackable certification credentials.	Level 2 certifications would already be accomplished in order to meet the minimum certifications required for the position of CISO; those certifications are not documented here. See map of stackable certification credentials.	An advanced certification (above Level 3) is recommended for this position: • (ISC)2 Information System Security Management Professional (CISSP-ISSMP) Level 3 certifications are listed below: • (ISC)2 Information Security System Professional (CISSP) • ISACA Certified Information Security Manager (CISM) • EC Council Certified Chief Information Security Officer (CCISO)	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 TRAINING • Attend annual threat intelligence training from SANS or other provider • Participate in annual incident response table-top scenario exercises • Complete (CFR) CyberSec First Responder: Threat Detection and Response (Exam CFR-210) • Attend training in cybersecurity governance, risk, and compliance • Maintain familiarity with cybersecurity operations, trends, and toolsets Advanced certification options include the following: • GIAC Security Expert (GSE) • (ISC)2 Information System Security Management Professional (CISSP-ISSMP) • Axelos ITIL Master

Oversee & Govern	Information Security Manager	Manages the agency cybersecurity program to include security awareness and training, maintains security strategies, incident response plans, and disaster recovery plans. This role is responsible for the cybersecurity of a program, organization, system, or enclave.	Current standing in one of the following certifications: • GIAC Security Leadership (GSLC) • (ISC)2 Certified Information Systems Security Professional (CISSP). • ISACA Certified Information Security Manager (CISM). Preferred qualification: Bachelor's degree in IT security management, information security, cybersecurity, or related discipline. Degree requirement may be waived based on professional experience.	Level 1 certifications would already be accomplished to meet the minimum certifications required for the position of an ISM; those certifications are not documented here. See map of stackable certification credentials.	Attain and maintain at least one of the following certifications: • GIAC Security Essentials Certification (GSEC) • EC Council Certified Ethical Hacker (CEH) • CompTIA Advanced Security Practitioner (CASP+)	• Mile2 Certified Information Systems Security Manager (CISSM) • IAPP Certified Information Privacy Manager (CIPM)	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 annual threat intelligence training from SANS (or other provider) • Participate in annual incident response table-top scenario exercises • Complete (CFR) CyberSec First Responder: Threat Detection and Response (Exam CFR-210) Recommend attaining specialty certifications relevant to the agency being supported. Examples include training/certifications in data privacy and regulatory controls, incident response, risk management, or infrastructure management.
Oversee & Govern	Risk/Compliance Manager	Performs risk assessments and establishes tolerance for risk based on mission, critical information systems infrastructure and efficacy of countermeasures / resilience. Quantifies residual risk.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in IT security management, information security, cybersecurity, or related discipline.	• CompTIA Security+ • (ISC)2 System Security Certified Practitioner (SSCP)	• GIAC Security Essentials Certification (GSEC) • ISACA Certified Information Security Auditor (CISA) • ISACA Certified in Risk & Information Systems Control (CRISC) • GRMI Certified Risk Management Professional (CRMP)	• PMI Project Management Professional-Risk Management Certification (PMP-RMC) • (ISC)2 Information System Security Professional (CISSP)	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 annual threat intelligence training from SANS (or other provider) • Participate in annual incident response table-top scenario exercises Recommend attaining one or more of the following specialty certifications such as: • GIAC Strategic Planning, Policy, and Leadership (GSTRT) • (ISC)2 Certified in Governance, Risk, and Compliance (CGRC) • PMI Project Management Professional (PMP) • (ISC)2 Information System Security Engineering Professional (CISSP-ISSEP)

Oversee & Govern	Cyber Policy Planner	Develops and maintains cybersecurity plans, policies, and strategy to support and align with enterprise cybersecurity initiatives and regulatory compliance.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in cybersecurity, IT security management, IT management, information security. Bachelor's degree in political science, business management, communications, or public administration may be acceptable WITH cybersecurity experience.	• CompTIA Security+ • (ISC)2 System Security Certified Practitioner (SSCP)	• GIAC Security Essentials Certification (GSEC) • CompTIA Advanced Security Practitioner (CASP+)	• GIAC Security Leadership (GSLC) • (ISC)2 Certified Information Systems 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 annual threat intelligence training from SANS (or other provider) • Complete (CFR) CyberSec First Responder: Threat Detection and Response (Exam CFR-210) • Participate in annual incident response table-top scenario exercises Recommend attaining one or more of the following specialty certifications such as: • GIAC Strategic Planning, Policy, and Leadership (GSTRT) • (ISC)2 Certified in Governance, Risk, and Compliance (CGRC) • ISACA Certified in Risk and Information Systems Control (CRISC) • PMI Project Management Professional (PMP)
Oversee & Govern	Cybersecurity Training Coordinator	Manages the cybersecurity training, education, and awareness program for the enterprise. Coordinates individual and group training opportunities; organizes cybersecurity color teams practices and captures effectivity metrics.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in cybersecurity, IT management, information security. Bachelor's degree in education, communications, or public administration may be acceptable WITH cybersecurity experience.	• CompTIA Security+ • (ISC)2 System Security Certified Practitioner (SSCP) • EC Council Certified Network Defender (CND)	• GIAC Security Essentials Certification (GSEC)	• GIAC Security Leadership (GSLC) • (ISC)2 Certified Information Systems 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 annual threat intelligence training from SANS (or other provider) • Attend instructional design/workforce training seminars • Attend MITRE ATT&CK training • Observe annual incident response table-top scenario exercises

Oversee & Govern	Business Process Analyst	Works within the organization and stakeholder entities to improve performance and processes using technology.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in business, economics, information systems, computer science, or related discipline.	• ABPMP Certified Business Process Associate (CBPA) • IIBA Certified Business Analysis Professional (CBAP) • Axelos IT Infrastructure Library (ITIL) Foundations	• Six Sigma Green Belt • ABPMP Certified Business Process Professional (CBPP)	• (ISC)2 Certified Information Security Professional (CISSP) • PMI Project Management Professional (PMP) • Six Sigma Black Belt • AICPA Certified Information Technology Professional (CITP)	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 conducting information security risk assessments • Attend training on data security and regulation Recommend attaining one or more of the following certifications: • CompTIA Security+ • (ISC)2 System Security Certified Practitioner (SSCP) • EC Council Certified Network Defender (CND) • GIAC Security Essentials Certification (GSEC)
Investigate	Network Forensics Analyst	Analyzes network traffic and investigates computer security incidents to derive useful information in support of network vulnerability mitigation.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in computer science, computer engineering, information systems, computer forensics, or related discipline.	Level 1 certifications would already be accomplished to meet the minimum certifications required for the position of a Network Forensic Analyst; those certifications are not documented here. See map of stackable certification credentials.	• GIAC Security Essentials (GSEC) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Security Practitioner (CASP+) • GIAC Certified Intrusion Analyst Certification (GCIA) • GIAC Certified Incident Handler (GCIH) • GIAC Global Industrial Cyber Security Professional (GICSP)	• GIAC Network Forensic Analyst (GNFA) • (ISC)2 Certified Cyber Forensics Professional (CCFP) • GIAC Certified Intrusion Analyst (GCIA)	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 • Participate in hands-on lab training for simulated attacks • Participate in capture-the-flag events • Attend MITRE ATT&CK training Recommend attaining one or more of the following specialty certifications such as • IACRB Certified Cyber Threat Hunting Professional (CCTHP) • GIAC Reverse Engineering Malware (GREM)

Investigate	Host Forensics Analyst	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/operating system vulnerability mitigation.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in computer science, computer engineering, information systems, computer forensics, or related discipline.	Level 1 certifications would already be accomplished in order to meet the minimum certifications required for the position of Host Forensics Analyst; those certifications are not documented here. See map of stackable certification credentials.	• GIAC Security Essentials (GSEC) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Security Practitioner (CASP+) • GIAC Certified Intrusion Analyst Certification (GCIA) • GIAC Certified Incident Handler (GCIH) • DFCB Digital Forensics Certified Associate (DCFA) • ISFCE Certified Computer Examiner (CCE)	• IACIS Certified Forensic Computer Examiner (CFCE) • GIAC Certified Forensic Analyst (GCFA) • GIAC Certified Forensic Examiner (GCFE)	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 • Participate in hands-on labs to maintain proficiency with Linux forensics, mobile forensics, iOS forensics • Participate in hands-on labs to learn techniques for forensic analysis within Industrial Control Systems (ICS) • Work toward Cloud certifications relevant to the enterprise environment The following are advanced specialty certifications which may interest an Expert Host Forensic Analyst: • GIAC Battlefield Forensics and Acquisition • GIAC Reverse Engineering Malware (GREM)
Investigate	Cloud Forensics Analyst	Uses forensic techniques to investigate cyber incidents in cloud environments.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in computer science, computer engineering, information systems, computer forensics, or related discipline.	Level 1 certifications would already be accomplished to meet the minimum certifications required for the position of Cloud Forensics Analyst; those certifications are not documented here. See map of stackable certification credentials.	• (ISC)2 Certified Cloud Security (CCSP) • AWS Certified Security • Microsoft Certified: Azure Fundamentals • Google Professional Cloud Security Engineer • GIAC Cloud Threat Detection (GCTD)	• (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 The following are advanced specialty certifications which may interest an Expert Cloud Forensic Analyst: • GIAC Battlefield Forensics and Acquisition • GIAC Reverse Engineering Malware (GREM)

Analyze	Penetration Tester	Performs penetration testing on web applications, networks, and infrastructure along with physical security reviews and social engineering tests to identify an organization's vulnerabilities and security weaknesses.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Associate's degree in computer science, computer engineering, software development, information systems, cybersecurity, or related discipline.	Level 1 certifications would already be accomplished to meet the minimum certifications required for the Penetration Tester; those certifications are not documented here. See map of stackable certification credentials.	• CompTIA PenTest+ • GIAC Certified Penetration Tester (GPEN) • EC Council Certified Ethical Hacker (CEH) • GIAC Certified Intrusion Analyst Certification (GCIA)	• EC Council Licensed Penetration Tester - Master (LPT) • GIAC Web Application Penetration Tester (GWAPT) • Offensive Security Certified Professional (OSCP)	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 OWASP training • Attend MITRE ATT&CK training • Attend annual threat intelligence training from SANS or other provider • Attend scripting or programming language training needed for environment
Analyze	Malware Analyst	Collaborates with network and host forensics analysts to collect malware and analyze the behavior and techniques used in the code to exploit systems.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in computer engineering, computer science, cybersecurity, programming, mathematics, or related field.	Level 1 certifications would already be accomplished to meet the minimum certifications required for the Malware Analyst; those certifications are not documented here. See map of stackable certification credentials.	• GIAC Certified Intrusion Analyst Certification (GCIA)	• Offensive Security Certified Professional (OSCP) • Offensive Security Exploitation Expert (OSEE) • Offensive Security Advanced Evasion Techniques and Breaching Defenses (OSEP) • GIAC Exploit Researcher & Advanced Penetration Tester (GXPN) • GIAC Reverse Engineering Malware Certification (GREM)	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 assembly language training to expanding knowledge of computer architecture and low-level programming Recommend attaining one or more of the following specialty certifications such as • C++ Certified Associate Programmer Certificate (CPA) • Python Institute Certified Associate in Python Programming (PCAP) • Oracle Certified Associate Java Programmer (OCAJP)

Analyze	Threat Intelligence Analyst	Analyzes cyber threat intelligence and indicators of compromise to communicate awareness of cyber threats throughout the business environment.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in cybersecurity, information technology, or a related discipline.	• CompTIA Security+ • (ISC)2 System Security Certified Practitioner (SSCP) • EC Council Certified Network Defender (CND)	• GIAC Security Essentials Certification (GSEC) • GIAC Cyber Threat Intelligence (GCTI) • EC Council Threat Intelligence Analyst (CTIA)	• (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 annual threat intelligence training from SANS or other provider • Attend MITRE ATT&CK training • Participate in annual incident response table-top scenario exercises Recommend attaining one or more of the following specialty certifications such as: • GIAC Certified Incident Handler (GCIH) • IACRB Certified Cyber Threat Hunting Professional (CCTHP) • GIAC Certified Intrusion Analyst Certification (GCIA)
Collect & Operate	Cybersecurity Analyst	Analyzes cybersecurity policies and protocols, conducts audits and risk assessments. Assesses security technology, monitors networks for security breaches and investigates when breaches occur. Researches latest cybersecurity trends and prepares reports of metrics for cyber incidents and attacks.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Associate's degree in cybersecurity, information technology, networking, or a related discipline.	• CompTIA Network+ • CompTIA Security+ • EC Council Cyber Network Defender (CND) • (ISC)2 System Security Certified Professional (SSCP)	• GIAC Security Essentials (GSEC) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Security Practitioner (CASP+) • ISACA Certified Information Systems Auditor (CISA) • GIAC Certified Enterprise Defender (GCED) • GIAC Certified Intrusion Analyst Certification (GCIA) • GIAC Certified Incident Handler (GCIH)	Level 3 certifications for a Cybersecurity Analyst depend on the career focus. See Level 3 certification in any of the Govern, Investigate, Analyze, or Protect & Defend workforce categories.	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 SIEM tools in use to gain advanced skills in creating dashboards and filtering data • Attend training on MITRE ATT&CK Framework • Attend training for NIST policies • Attend training for privacy regulation and identity access management (IAM) best practices Recommend attaining one or more of the following specialty certifications such as • (ISC)2 Information Systems Security Engineer (CISSP-ISSEP)

Collect & Operate	Systems Analyst	Responsible for analyzing, modifying, designing, and managing IT systems and networks for the organization or its affiliated agencies / clients.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in computer science, computer engineering, information systems, cybersecurity or related discipline.	• CompTIA A+ • CompTIA Network+ • CompTIA Security+ • EC Council Certified Network Defender (CND) • (ISC)2 System Security Certified Professional (SSCP) • Axelos IT Information Library Foundations (ITIL)	• GIAC Security Essentials (GSEC) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Security Practitioner (CASP+) • ISACA Certified Information Systems Auditor (CISA) • GIAC Certified Enterprise Defender (GCED)	• (ISC)2 Certified Information Security Professional (CISSP) • ISACA Certified Information Security Manager (CISM) • PMI Project Management Professional (PMP)	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 annual threat intelligence training from SANS (or other provider) • Attend Systems Development Lifecycle (SDLC) training Recommend attaining one or more of the following specialty certifications such as • PMI Agile Certified Practitioner (ACP) • PMI Certified Scrum Master (CSM) • GIAC Certified Incident Handler (GCIH) • GIAC Certified Intrusion Analyst Certification (GCIA)
Collect & Operate	SIEM Engineer	Configure and customize Security Information and Event Management (SIEM), Data Loss Prevention (DLP), and Intrusion Detection/Prevention System (IDS/IPS) tools. Review suspicious patterns and signatures and write custom scripts to detect malware and eliminate network noise.	Recommend vendor-specific certifications focused on technology in use the environment such as Splunk, QRadar, or other SIEM toolset. Preferred qualification: Bachelor's degree in computer science, computer engineering, information systems, cybersecurity, or related discipline.	Level 1 certifications would already be accomplished to meet the minimum certifications required for the SIEM Engineer; those certifications are not documented here. See map of stackable certification credentials.	• CompTIA Cybersecurity Analyst (CySa+) • CompTIA Advanced Security Practioner (CASP+) • GIAC Defensible Security Architect (GDSA) • GIAC Certified Enterprise Defender (GCED) • EC Council Certified SOC Analyst (CSA) • SBT Blue Team Level 2 (BTL2) • GIAC Certified Intrusion Analyst Certification (GCIA)	• SBT Certified Security Operations Manager (CSOM) • (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 annual threat intelligence training from SANS (or other provider) • Maintain vendor-specific training depending on environment such as Splunk or QRadar. • Attend training on MITRE ATT&CK Framework • Attend SANS SEC555: SIEM with Tactical Analytics or similar course Recommend attaining one or more of the following specialty certifications such as • GIAC Certified Incident Handler (GCIH) • EC Council Certified Incident Handler (ECIH) • IACRB Certified Cyber Threat Hunting Professional (CCTHP)

Collect & Operate	DevSecOps Engineer	Creates and maintains secure systems with a focus on integrating security throughout the development lifecycle. Works with stakeholders to ensure systems are protected from potential threats and vulnerabilities.	Recommend vendor-specific certifications focused on technology in use the environment (such as AWS, Azure, or RedHat), Recommend certifications in deployment tools such as Puppet, Terraform, and Chef. Preferred qualification: Bachelor's degree in computer science, computer engineering, information technology, cybersecurity or related discipline.	Level 1 certifications would already be accomplished in order to meet the minimum certifications required for the SIEM Engineer; those certifications are not documented here. See map of stackable certification credentials.	• GIAC Defensible Security Architect (GDSA) • GIAC Certified Enterprise Defender (GCED) • Puppet Certified Professional • Certified Kubernetes Administrator (CKA) • Docker Certified Associate (DCA) • Jenkins Certified Engineer	• AWS Certified DevOps Engineer • Azure DevOps Engineer • RedHat Certified Engineer in DevOps Automation	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 security training for development within the Software/Systems Development Lifecycle (SDLC) • Attend training on security development for Cloud infrastructures (i.e. Kubernetes Security Specialist) Recommend attaining one or more of the following specialty certifications such as • PMI Agile Certified Practitioner (ACP) • PMI Certified Scrum Master (CSM) • (ISC)2 Certified Cloud Security Professional (CCSP) • GIAC Certified Incident Handler (GCIH)
Collect & Operate	Application Developer	Creates, tests, programs, and maintains cybersecurity software, utilities, and tools for a specific device, operating system, or client/purpose.	Recommend vendor-specific certifications focused on technology in use the environment (such as Python, C/C++, Java). Should be familiar with Git, API development, data structures and algorithms, and cloud infrastructures. Recommended cybersecurity certifications are listed by level on the right. Preferred qualification: Bachelor's degree in software engineering, computer science, cybersecurity, information technology, or a related discipline.	• CompTIA Security+ • EC Council Certified Network Defender (CND) • (ISC)2 System Security Certified Professional (SSCP)	• EC Council Certified Secure Programmer (ECSP) • EC Council Certified Secure Application Developer (CSAD) • (ISC)2 Certified Secure Software Lifecycle Professional (CSSLP)	• IEEE Certified Software Development Professional (CSDP) • IEEE Software Engineering Master Certification (SEMC).	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 for Software Development Lifecycle (SDLC) Recommend attaining one or more of the following specialty certifications such as • PMI Agile Certified Practitioner (ACP)

Protect & Defend	Cyber Operations Coordinator	Direct CSOC operations, responsible for syncing between analysts and engineers; hiring; training; and creating and executing on cybersecurity strategy. Direct and orchestrate the responses to cybersecurity threats.	Current standing in at least TWO of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in cybersecurity, information technology, networking, or a related discipline.	• CompTIA Network+ • CompTIA Security+ • EC Council Cyber Network Defender (CND) • (ISC)2 System Security Certified Professional (SSCP) • CompTIA Cloud+	• EC Council Certified Ethical Hacker (CEH) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Security Practitioner (CASP+) • EC Council Certified Incident Handler (ECIH) • GIAC Certified Incident Handler (GCIH) • GIAC Certified Detection Analyst (GCDA) • SBT Blue Team Level 1 (BTL1)	• SBT Blue Team Level 2 (BTL2) • SBT Certified Security Operations Manager (CSOM) • Mile2 Certified Incident Handling Engineer (CIHE) • GIAC Security Leadership (GSLC) • (ISC)2 Information Security System 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 USG CISA Incident Response Training (IRT) • Attend annual threat intelligence training from SANS or other provider • Participate in annual incident response table-top scenario exercises • Complete (CFR) CyberSec First Responder: Threat Detection and Response (Exam CFR-210) • Attend Public Relations/Communications training for Incident Response Recommend attaining one or more of the following specialty certifications such as • Mile2 Certified Disaster Recovery Specialist (CDRE) • GIAC Battlefield Forensics & Acquisition (GBFA)
Protect & Defend	SIEM Analyst	Monitors and analyzes network security sensors to identify, triage, remediate, or escalate cyber incidents. Maintains and tunes security rule, queries, and filters for collection within the Security Information and Even Management (SIEM) toolset.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Associate's degree in cybersecurity, information technology, networking, or a related discipline.	• CompTIA Network+ • CompTIA Security+ • EC Council Cyber Network Defender (CND) • (ISC)2 System Security Certified Professional (SSCP)	• EC Council Certified Ethical Hacker (CEH) • CompTIA Cybersecurity Analyst (CySa+) • CompTIA Advanced Security Practioner (CASP+) • GIAC Certified Enterprise Defender (GCED) • EC Council Certified SOC Analyst (CSA) • SBT Blue Team Level 1 (BTL1) • EC Council Certified Incident Handler (ECIH) • GIAC Certified Intrusion Analyst Certification (GCIA)	• SBT Blue Team Level 2 (BTL2) • SBT Certified Security Operations Manager (CSOM) • (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 digital or network forensics training • Attend incident response training • Attend vendor-specific training on security infrastructure toolsets for IDS/IPSs and SIEMs, and vulnerability scanning tools in use in the environment. • Participate in Capture-the-Flag events Recommend attaining one or more of the following specialty certifications such as • GIAC Network Forensic Analyst (GNFA) • DFCB Digital Forensics Certified Associate (DCFA) • IACRB Certified Cyber Threat Hunting Professional (CCTHP)

Protect & Defend	Senior Incident Responder	Supports end-to-end incident response process for the enterprise including analysis, containment, eradication, recovery, and stakeholder communications. Develops and oversees cybersecurity metrics to measure operational effectiveness to drive improvement.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in cybersecurity, information security, or a related discipline. Bachelor's degree in political science, business management, communications, or public administration may be acceptable WITH cybersecurity experience.	Level 1 certifications would already be accomplished to meet the minimum certifications required for the Senior Incident Responder; those certifications are not documented here. See map of stackable certification credentials.	• CompTIA Cybersecurity Analyst (CySa+) • CompTIA Advanced Security Practioner (CASP+) • GIAC Certified Enterprise Defender (GCED) • EC Council Certified Incident Handler (ECIH) • GIAC Certified Incident Handler (GCIH) • GIAC Certified Intrusion Analyst Certification (GCIA) • CertNexus CyberSec First Responder: Threat Detection and Response (CFR) • SBT Blue Team Level 2 (BTL2)	• Mile2 Certified Incident Handling Engineer (CIHE) • (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 USG CISA Incident Response Training (IRT) • Attend annual threat intelligence training from SANS or other provider • Complete (CFR) CyberSec First Responder: Threat Detection and Response (Exam CFR-210) • Participate in annual incident response table-top scenario exercises • Attend Public Relations/Communications training for Incident Response Recommend attaining one or more of the following specialty certifications such as • Mile2 Certified Disaster Recovery Specialist (CDRE) • GIAC Battlefield Forensics & Acquisition (GBFA)
Protect & Defend	Incident Responder	Responsible for monitoring and analyzing an organization's network and systems for security threats and vulnerabilities. Detects and responds to cybersecurity incidents covering all phases of attack to include containment and eradication. Analyzes cybersecurity incidents and escalates responses to the CSIRT as needed.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Associate's degree in cybersecurity, information security, or a related discipline. A degree in political science, business management, communications, or public administration may be acceptable WITH cybersecurity experience.	• CompTIA Security+ • EC-Council Certified Network Defender (CND)	• EC Council Certified Ethical Hacker (CEH) • SBT Blue Team Level 1 (BTL1) • CompTIA Cybersecurity Analyst (CySa+) • CompTIA Advanced Security Practioner CE (CASP) • GIAC Certified Enterprise Defender (GCED) • EC Council Certified Incident Handler (ECIH) • GIAC Certified Incident Handler (GCIH) • SBT Blue Team Level 1 (BTL1)	• SBT Blue Team Level 2 (BTL2) • Mile2 Certified Incident Handling Engineer (CIHE)	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 SIEM tools in use, traffic analysis, • Attend training on MITRE ATT&CK Framework • Complete (CFR) CyberSec First Responder: Threat Detection and Response (Exam CFR-210) Recommend attaining one or more of the following specialty certifications such as • GIAC Network Forensic Analyst (GNFA) • (ISC)2 Certified Cyber Forensics Professional (CCFP) • GIAC Certified Intrusion Analyst (GCIA) • GIAC Global Industrial Cyber Security Professional (GICSP)

Operate & Maintain	Helpdesk	Serves as the first point of contact for customers seeking technical assistance via phone or email, performs remote troubleshooting through diagnostic techniques and asking pertinent questions. Determines the best solution to resolve the issue or escalates the issue to more experienced resources.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Associate's degree in cybersecurity, information technology, or a related discipline.	• CompTIA A+ • CompTIA Network+ • CompTIA Security+ • ITIL Foundations • Microsoft 365: Certified Endpoint Administrator 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 training on specific tools and applications used within the environment such as specialty printers, virtual machines, or operating systems other than Windows. Recommend attaining one or more of the following specialty certifications such as • CompTIA Linux+ • CompTIA Server+ • CompTIA Cloud+
Operate & Maintain	Network Technician	Monitors and analyzes network traffic to identify and resolve cyber threats. Configures, maintains, and troubleshoots routers, switches, firewalls, and other network and security devices.	Current standing in at least TWO of the following certifications based on certification levels noted to the right. Preferred qualification: Associate's degree in cybersecurity, information technology, network technology, or a related discipline.	• CompTIA A+ • CompTIA Network+ • Cisco Certified Technician (CCT) • CompTIA Security+ • CompTIA Linux+ • CompTIA Cloud+ • EC-Council Certified Network Defender (CND) • (ISC)2 System Security Certified Practitioner (SSCP)	• Cisco Certified Network Associate (CCNA) • Cisco Certified CyberOps Associate (CCNA-CyberOps) • EC Council Network Security Administrator (ENSA)	• Cisco Certified Network Professional - Enterprise (CCNP)	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 how to secure specific tools and applications used within the environment such as vendor-specific firewalls, Juniper networks, or cloud configurations. Recommend attaining one or more of the following specialty certifications such as • AWS Cloud Practitioner • Azure Cloud Fundamentals • Google Cloud Digital Leader

Operate & Maintain	Network Administrator	Develops, manages, and maintains network infrastructure to include documentation of policies, procedures, inventory, and performance metrics.	Current standing in at least TWO of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in cybersecurity, information technology, network technology, or a related discipline.	• CompTIA A+ • CompTIA Network+ • Cisco Certified Technician (CCT) • CompTIA Security+ • CompTIA Linux+ • CompTIA Cloud+ • EC-Council Certified Network Defender (CND) • (ISC)2 System Security Certified Practitioner (SSCP)	• Cisco Certified Network Associate (CCNA) • Cisco Certified CyberOps Associate (CCNA-CyberOps) (CCNA-CyberOps) • EC Council Network Security Administrator (ENSA)	• Cisco Certified Network Professional - Enterprise (CCNP)	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 Security Essentials for IT Administrators (offered by SANS, but similar content is available from other vendors) • Attend cloud security training in relevant enterprise cloud infrastructure Recommend attaining one or more of the following specialty certifications such as • VMware Certified Professional (VCP) • (ISC)2 Certified Cloud Security Professional (CCSP)
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.	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. Preferred qualification: Bachelor's degree in computer science, cybersecurity, information technology, or a related discipline.	• 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.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's Degree in computer science, information science, technical writing, or a related analytics field.	• 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 Security 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 Recommend attaining one or more of the following specialty certifications such as • EC Council Certified Ethical Hacker (CEH) • DAMA Certified Data Management Professional (CDMP) • PMI Project Management Professional (PMP)
Operate & Maintain	Compliance Analyst	Ensures enterprise operations and procedures meet appropriate local, federal, and state laws and regulation. Examines and develops policies and procedures, identifies areas out of compliance, and advises on methods for necessary modifications.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in IT security management, information security, cybersecurity, or related discipline.	• CompTIA Security+ • (ISC)2 System Security Certified Practitioner (SSCP)	• GIAC Security Essentials Certification (GSEC) • ISACA Certified Information Security Auditor (CISA) • ISACA Certified in Risk & Information Systems Control (CRISC) • GRMI Certified Risk Management Professional (CRMP)	• PMI Project Management Professional-Risk Management Certification (PMP-RMC) • (ISC)2 Information System Security Professional (CISSP) • (ISC)2 Information System Security Engineering Professional (CISSP-ISSEP)	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 controls Recommend attaining one or more of the following specialty certifications such as: • GIAC Strategic Planning, Policy, and Leadership (GSTRT) • (ISC)2 Certified in Governance, Risk, and Compliance (CGRC) • PMI Project Management Professional (PMP)

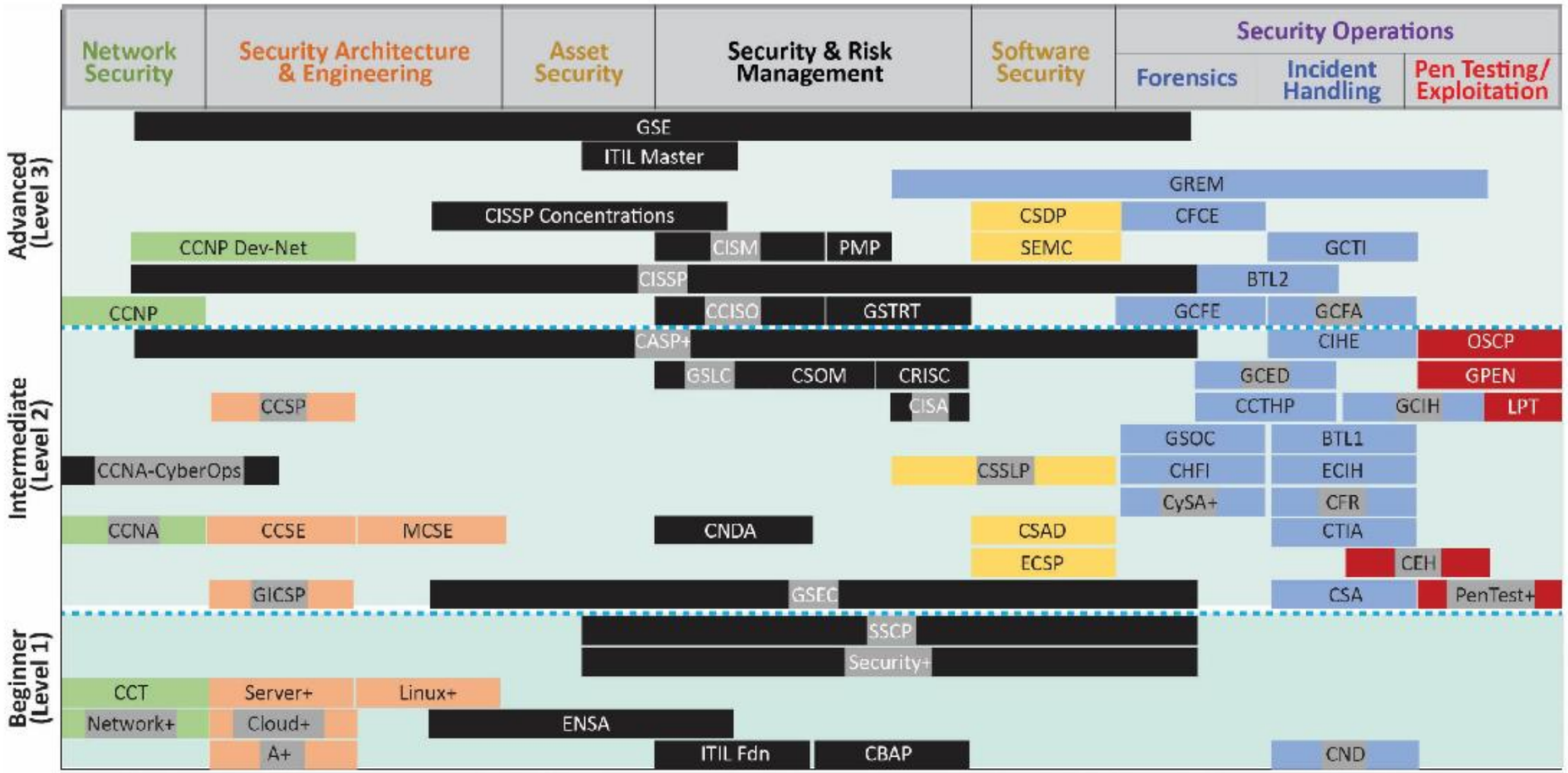
Operate & Maintain	Vulnerability Assessment Analyst	Performs assessments of systems and networks within the enterprise environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Analyzes vulnerabilities and prioritizes based on impact.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Associate's degree in IT security management, information security, cybersecurity, or related discipline.	• CompTIA A+ • CompTIA Network+ • Cisco Certified Technician (CCT) • CompTIA Security+ • CompTIA Cloud+ • EC-Council Certified Network Defender (CND) • (ISC)2 System Security Certified Practitioner (SSCP)	• GIAC Security Essentials Certification (GSEC) • Cisco Certified Network Associate (CCNA) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Security Practitioner (CASP+) • ISACA Certified Information Systems Auditor (CISA)	• Cisco Certified Network Professional (CCNP) • (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 vendor-based training for vulnerability scanning tools in use. • Attend vendor-based training on infrastructure technology in use such as firewalls, switches, and routers. Recommend attaining one or more of the following specialty certifications such as • GIAC Certified Enterprise Defender (GCED) • GIAC Certified Incident Handler (GCIH) • GIAC Enterprise Vulnerability Assessor • NICCS Certified Vulnerability Assessor (CVA)
Operate & Maintain	DevSecOps Engineer	Creates and maintains secure systems with a focus on integrating security throughout the development lifecycle. Works with stakeholders to ensure systems are protected from potential threats and vulnerabilities.	Recommend vendor-specific certifications focused on technology in use the environment (such as AWS, Azure, or RedHat), Recommend certifications in deployment tools such as Puppet, Terraform, and Chef. Preferred qualification: Bachelor's degree in computer science, computer engineering, information technology, cybersecurity or related discipline.	Level 1 certifications would already be accomplished in order to meet the minimum certifications required for the SIEM Engineer; those certifications are not documented here. See map of stackable certification credentials.	• Puppet Certified Professional • Certified Kubernetes Administrator (CKA) • Docker Certified Associate (DCA) • Jenkins Certified Engineer	• AWS Certified DevOps Engineer • Azure DevOps Engineer • RedHat Certified Engineer in DevOps Automation	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 security training for development within the Software/Systems Development Lifecycle (SDLC) • Attend training on security development for Cloud infrastructures (i.e. Kubernetes Security Specialist) Recommend attaining one or more of the following specialty certifications such as • PMI Agile Certified Practitioner (ACP) • PMI Certified Scrum Master (CSM) • (ISC)2 Certified Cloud Security Professional (CCSP) • GIAC Certified Incident Handler (GCIH)

Securely Provision	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.	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. Preferred qualification: Bachelor's degree in computer science, cybersecurity, information technology, or a related discipline.	• 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+)	• (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
Securely Provision	Application Architect	Designs major aspects of an application including components such as user interface, middleware, and infrastructure. Provides technical leadership to the application development team; performs code review and ensures enterprise-wide application design standards are maintained.	Recommend vendor-specific certifications focused on technology in use the environment (such as Python, C/C++, Java, .NET, PHP). Should be familiar with Git, API development, data structures and algorithms, and cloud infrastructures, and SDLC. Recommended cybersecurity certifications are listed by level on the right. Preferred qualification: Bachelor's degree in software engineering, computer science, cybersecurity, information technology, or a related discipline.	Level 1 certifications would already be accomplished in order to meet the minimum certifications required for the Application Architect; those certifications are not documented here. See map of stackable certification credentials.	• EC Council Certified Secure Programmer (ECSP) • EC Council Certified Secure Application Developer (CSAD) • (ISC)2 Certified Secure Software Lifecycle Professional (CSSLP)	• IEEE Certified Software Development Professional (CSDP) • IEEE Software Engineering Master Certification (SEMC).	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 OWASP training • Attend MITRE ATT&CK training • Attend training in secure coding principles, techniques, and best practices Recommend attaining one or more of the following specialty certifications such as • PMI Agile Certified Practitioner (ACP)

Securely Provision	Application Developer	Creates, tests, programs, and maintains cybersecurity software, utilities, and tools for a specific device, operating system, or client/purpose.	Recommend vendor-specific certifications focused on technology in use the environment (such as Python, C/C++, Java). Should be familiar with Git, API development, data structures and algorithms, and cloud infrastructures. Recommended cybersecurity certifications are listed by level on the right. Preferred qualification: Bachelor's degree in software engineering, computer science, cybersecurity, information technology, or a related discipline.	• CompTIA Security+ • EC Council Certified Network Defender (CND) • (ISC)2 System Security Certified Professional (SSCP)	• EC Council Certified Secure Programmer (ECSP) • EC Council Certified Secure Application Developer (CSAD) • (ISC)2 Certified Secure Software Lifecycle Professional (CSSLP)	• IEEE Certified Software Development Professional (CSDP) • IEEE Software Engineering Master Certification (SEMC).	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 Software Development Lifecycle (SDLC) training • Attend training in secure coding principles, techniques, and best practices • Attend training in Agile/Scrum/DevOps Recommend attaining one or more of the following specialty certifications such as • PMI Agile Certified Practitioner (ACP)
Securely Provision	Security Architect	Plans and designs resilient security architectures for various IT projects based on stakeholder needs. Develops prerequisites for networks, firewalls, routers, and other network devices, then implements solutions with updated security standards, systems, and best practices.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in computer science, computer engineering, information technology, cybersecurity, or related discipline.	• CompTIA A+ • CompTIA Network+ • Cisco Certified Technician (CCT) • CompTIA Security+ • CompTIA Cloud+ • EC-Council Certified Network Defender (CND) • (ISC)2 System Security Certified Practitioner (SSCP)E	• GIAC Security Essentials Certification (GSEC) • Cisco Certified Network Associate (CCNA) • Cisco Certified Network Professional (CCNP) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Security Practitioner (CASP+) • ISACA Certified Information Systems Auditor (CISA)	• CREST Registered Technical Security Architect (CRTSA) • The Open Group Architecture Framework (TOGAF) certification • (ISC)2 Information System Security Architect Professional (CISSP-ISSAP)	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 such as • GIAC Certified Enterprise Defender (GCED) • GIAC Certified Incident Handler (GCIH) • GIAC Enterprise Vulnerability Assessor • NICCS Certified Vulnerability Assessor (CVA) • (ISC)2 Information System Security Architect Professional (CISSP-ISSAP)

Securely Provision	Security Engineer	Works closely with cross-functional teams, including IT, network engineering, and cybersecurity, to ensure that systems and networks are secure, compliant with applicable regulations, and protected against unauthorized access and other security risks.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in computer science, computer engineering, information technology, cybersecurity or related discipline.	Level 1 certifications would already be accomplished to meet the minimum certifications required for the Security Engineer; those certifications are not documented here. See map of stackable certification credentials.	• GIAC Security Essentials Certification (GSEC) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Security Practitioner (CASP+) • ISACA Certified Information Systems Auditor (CISA) • (ISC)2 Certified Cloud Security Professional (CCSP)	• Cisco Certified Network Professional (CCNP) • Cisco Certified Network Professional - DevNet Professional (CCNP-DevNet)	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 • Maintain awareness of NIST, ISO 27001, and CIS Critical Security Controls documentation and guidance • Attend vendor-specific training on security infrastructure toolsets for IDS/IPSs, SIEMs, and vulnerability scanning tools in use in the environment. Recommend attaining one or more of the following specialty certifications such as • PMI Project Management Professional (PMP) • EC Council Certified Ethical Hacker (CEH) • GIAC Certified Enterprise Defender (GCED) • GIAC Certified Incident Handler (GCIH) • GIAC Global Industrial Cyber Security Professional (GICSP)

Appendix C – Stackable Certification Map



Certifications highlighted in gray meet DoD 8570 baseline certification requirements. See the full list of DoD approved certifications at https://public.cyber.mil/wid/cwmp/dod-approved-8570-baseline-certifications/

A.2 F.S. 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.—

(a) The Florida Digital Service shall:

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.—

(a) Each local government shall adopt cybersecurity standards that safeguard its data, information 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.—

(a) A local government shall provide notification of a cybersecurity incident or ransomware incident to the Cybersecurity Operations Center, Cybercrime Office of the Department of Law Enforcement, 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.

5. In the case of a ransomware incident, the details of the ransom demanded.

6. A statement requesting or declining assistance from the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, or the sheriff who has jurisdiction over the local government.

(b)1. A local government shall report all ransomware incidents and any cybersecurity incident determined by the local government to be of severity level 3, 4, or 5 as provided in s. 282.318(3)(c) to the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government as soon as possible but no later than 48 hours after discovery of the cybersecurity incident and no later than 12 hours after discovery of the ransomware incident. The report must contain the information required in paragraph (a).

2. The Cybersecurity Operations Center shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incident as soon as possible but no later than 12 hours after receiving a local government's incident report. The notification must include a high-level description of the incident and the likely effects.

(c) A local government may report a cybersecurity incident determined by the local government to be of severity level 1 or 2 as provided in s. 282.318(3)(c) to the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government. The report shall contain the information required in paragraph (a).

(d) The Cybersecurity Operations Center shall provide a consolidated incident report on a quarterly basis to the President of the Senate, the Speaker of the House of Representatives, and the Florida Cybersecurity Advisory Council. The report provided to the Florida Cybersecurity Advisory Council may not contain the name of any local government, network information, or system identifying information but must contain sufficient relevant information to allow the Florida Cybersecurity Advisory Council to fulfill its responsibilities as required in s. 282.319(9).

(6) AFTER-ACTION REPORT.—A local government must submit to the Florida Digital Service, within 1 week after the remediation of a cybersecurity incident or ransomware incident, an after-action report that summarizes the incident, the incident's resolution, and any insights gained as a result of the incident. By December 1, 2022, the Florida Digital Service shall establish guidelines and processes for submitting an after-action report.

A.3 FL[DS] RESPONSIBILITY BREAKDOWNS

Section	Subsection	Party Responsible	Responsibility
282.3185	(3)(a)1	FL[DS]	Develop a basic cybersecurity training curriculum for local government employees.
282.3185	(3)(a)2	FL[DS]	Develop an advanced cybersecurity training curriculum for local governments which is consistent with the cybersecurity training required under s. 282.318(3)(g).
282.3185	(5)(b)(2)	FL[DS]	The Cybersecurity Operations Center shall notify the President of the Senate and the Speaker of the House of Representatives of any severity level 3, 4, or 5 incidents as soon as possible but no later than 12 hours after receiving a local government's incident report.
282.3185	(5)(d)	FL[DS]	The Cybersecurity Operations Center shall provide a consolidated incident report on a quarterly basis to the President of the Senate, the Speaker of the House of Representatives, and the Florida Cybersecurity Advisory Council.

A.4 ADDITIONAL RESOURCE LINKS

NIST Cybersecurity Framework Policy Template Guide

https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/img/uploads/2021/11/NIST-Cybersecurity-Framework-Policy-Template-Guide-v2111Online.pdf

CIS Center for Internet Security

https://www.cisecurity.org/

National Institute of Standards and Technology

https://www.nist.gov/

Free Cybersecurity Services and Tools | CISA

https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools

Training | Cyber Florida: The Florida Center for Cybersecurity

https://cyberflorida.org/cybersecureflorida/training/

A.5 F.S. 282.3185 QUICK REFERENCE – TEAR OUT

- General Information and latest Local Resource Packet
    - http://digital.fl.gov/cyber
- Training:
    - 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.
    - 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.
- Standards:
    - Each local government shall adopt cybersecurity consistent with generally accepted best practices for cybersecurity.
    - Visit digital.fl.gov/localgovernment-attestation-form to submit an online attestation, affirming your compliance.
- Incident Response:
    - All Ransomware and/or Incidents of severity level 3, 4, or 5 reported within 48 hours.
    - Local governments can request IR assistance, and FL[DS] will strive to provide full support.
        - IR.Digital.FL.gov – preferred method for Incident Reporting
        - CSOC@Digital.FL.gov
        - CSOC Phone: (850) 412-6074

A.6 INCIDENT REPORTING PROCESS – TEAR OUT

Three Ways to Contact Us

IR.Digital.FL.gov – preferred method for Incident Reporting

CSOC@Digital.FL.gov

CSOC Phone: (850) 412-6074

IR.digital.fl.gov

Reporting to Law Enforcement

- The FL[DS] Cybersecurity Operations Center (CSOC) reports all incidents to FDLE.
- The CSOC will work with your organization and FDLE to coordinate notification to local law enforcement.

Incident Severity Levels:

- Level 5 is an emergency-level incident that poses an imminent threat to life, wide-scale critical infrastructure, or national, state, or local government security.
- Level 4 is a severe-level incident likely to result in significant impact to public health, safety, liberty, economic security or public confidence.
- Level 3 is a high-level incident likely to result in demonstrable impact to public health, safety, liberty, economic security or public confidence.
- Level 2 is a medium-level incident that may impact to public health, safety, liberty, economic security or public confidence.
- Level 1 is a low-level incident that is unlikely to impact to public health, safety, liberty, economic security or public confidence.

Timeframes, Breach Reporting and Assistance:

- Report all ransomware incidents and any level 3, 4, or 5 cybersecurity incidents as soon as possible but no later than 48 hours after discovery of the cybersecurity incident and no later than 12 hours after discovery of the ransomware incident.
- Local governments can request IR assistance, and FL[DS] will strive to provide support.
- Any security breach affecting 500 or more individuals in Florida must be provided to the Department of Legal Affairs within 30 days as prescribed in F.S. 501.171(3).