2025 V2.0

THE LOCAL GOVERNMENT CYBERSECURITY RESOURCE PACKET

A Core Resource for
Local & State Government
Cybersecurity Collaboration
In the State of Florida

Florida Digital

Florida Digital Service
2555 Shumard Oak Blvd • Tallahassee, FL 32399
www.digital.fl.gov

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 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.

A Word from the Florida Digital Service

Local Partners & Colleagues,

It is our collective responsibility to help secure the information of more than 22 million Floridians. At the Florida Digital Service, we take this responsibility seriously and remain committed to supporting efforts that protect the confidentiality, integrity, and availability of data across our state.

We recognize that each local government faces unique challenges and priorities in serving its constituents. Whether you're a small town or a large municipality, your efforts play a vital role in strengthening our overall cybersecurity posture.

Trust and collaboration are at the core of our work. We understand the importance of building strong partnerships and maintaining open communication. Your dedication and continued engagement are essential to the success of our shared mission.

On behalf of our entire team at FLDS, thank you for your commitment to safeguarding your communities. We are grateful for your partnership and look forward to continuing our work together to protect the privacy and security of all Floridians.

With appreciation,
Florida Digital Service

Section 1: Information Security Program

1.1 Overview of Information Security Management

Effective information security management is essential for safeguarding systems, data, and critical services against cyber threats. A well-structured approach enables organizations to govern security, identify and mitigate risks, and implement measures to protect, detect, respond to, and recover from cyber incidents, while ensuring the confidentiality, integrity, and availability of information.

Key Components of an Information Security Program:

- Risk Assessment: Identifying threats, vulnerabilities, and potential impacts on information systems.
- Security Controls: Implementing technical, administrative, and physical measures to protect systems and data.
- Security Awareness and Training: Ensuring that employees understand their roles in protecting sensitive information.
- Incident Response and Recovery: Developing plans and capabilities to quickly respond to and recover from cybersecurity incidents.
- Continuous Monitoring: Regularly assessing security posture, detecting threats, and improving defenses.
- Governance and Compliance: Establishing policies, procedures, and oversight to align with industry best practices and regulatory requirements.

1.2 Frameworks for Information Security Management

There are multiple cybersecurity frameworks that organizations can use to establish and maintain a strong security program. Local governments may choose the framework that best fits their needs, compliance obligations, and risk management approach.

At the Florida Digital Service, we follow the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 as a guiding structure for cybersecurity strategy and risk management. NIST CSF 2.0 provides a flexible, scalable, and outcome-driven approach to managing cybersecurity risk.

The framework is built around six core functions:

- Govern – Establishes security strategy, roles, and oversight.
- Identify – Helps organizations understand risks, assets, and threats.
- Protect – Implements safeguards to reduce cybersecurity risks.
- Detect – Enables timely identification of cybersecurity events.
- Respond – Establishes processes for incident response and containment.
- Recover – Supports-- systems restoration and resilience after an incident.

Local governments are not required to use NIST CSF 2.0, but adopting a structured framework, whether NIST CSF, ISO 27001, CIS Controls, or another recognized model, can help enhance cybersecurity preparedness, compliance, and risk management.

For more information on security frameworks, visit:

- https://www.nist.gov/cyberframework
- https://www.cisecurity.org/controls
- https://www.iso.org/isoiec-27001-information-security.html

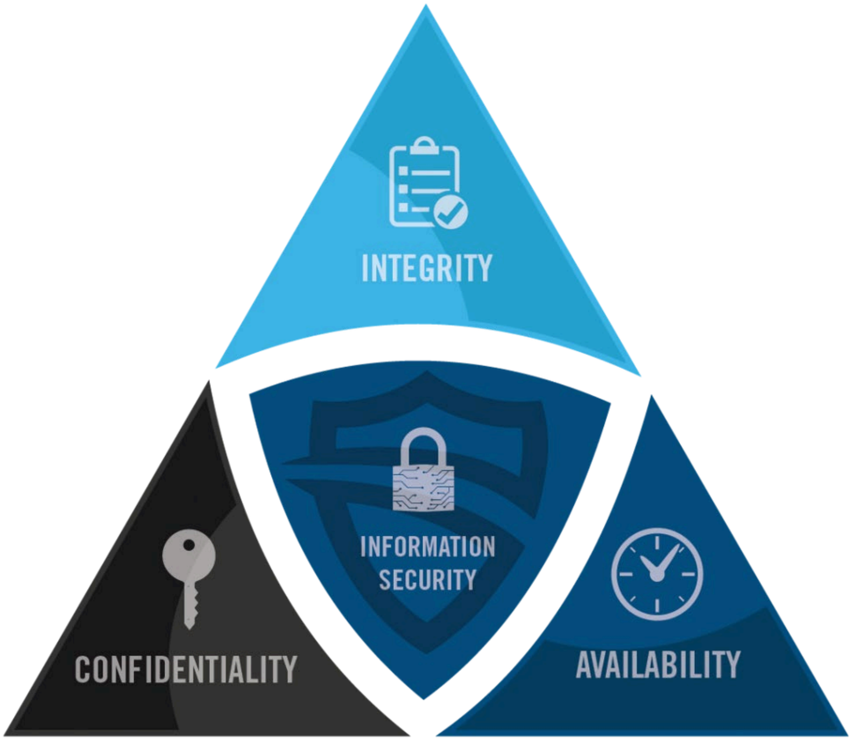
1.3 Importance of Information Security

In today's interconnected world, information security is critical for protecting sensitive data, maintaining public trust, and ensuring the resilience of government operations. Cyber threats, such as ransomware, data breaches, and phishing attacks, can disrupt essential services, compromise confidential information, and result in financial and reputational damage.

A strong cybersecurity posture helps organizations:

- Protect Confidentiality – Prevent unauthorized access to sensitive information.
- Ensure Integrity – Safeguard data from unauthorized changes or corruption.
- Maintain Availability – Ensure critical systems and services remain operational.

By implementing robust security measures, local governments can reduce risks, enhance public trust, and strengthen operational continuity in the face of evolving cyber threats. A proactive approach to cybersecurity supports long-term resilience and ensures that government agencies can continue to serve their communities effectively.



1.4 Roles and Responsibilities

Below is a list of common cybersecurity roles responsible for implementing and managing cybersecurity programs, securing digital assets, and defending against cyber threats.

State of Florida Chief Information Security Officer (CISO):

- Govern: Establishes governance structures for cybersecurity across the state, ensuring clear roles, responsibilities, and accountability. Leads the development of statewide cybersecurity governance frameworks that include policy formation, compliance oversight, and strategic planning in alignment with the state's objectives.
- 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

- Govern: Oversees the governance of cybersecurity audit and compliance programs. Ensures that cybersecurity audits are conducted in accordance with governance frameworks, and that findings are used to inform policy and strategy. Provides guidance on the governance aspects of cybersecurity to state agencies, including compliance with laws and regulations.
- 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

- Govern: Develops cybersecurity policies tailored to agency/local government needs.
- Identify: Leads risk assessments and ensures critical assets are protected.
- Protect: Implements security programs and ensures compliance with established frameworks.
- Detect: Monitors security threats and ensures effective detection mechanisms are in place.
- Respond: Leads incident response efforts within their agency/local government in coordination with the State CISO.
- Recover: Oversees recovery strategies to restore affected services and operations.

State and Local Information Security Managers

- Govern: Supports agency-wide cybersecurity governance efforts.
- Identify: Works with leadership to assess risks and prioritize security initiatives.
- Protect: Implements security measures, ensuring proper controls are in place.
- Detect: Oversees daily security operations, including vulnerability management.
- Respond: Acts as the first responder for cybersecurity incidents within the organization.
- Recover: Helps restore and validate system functionality for business operations after an event.

State and Local Inspectors General

- Govern: Conducts oversight of cybersecurity compliance.
- Identify: Audits current systems to identify vulnerabilities or compliance issues.
- Protect: Recommends security improvements based on audits.
- Detect: Reviews cybersecurity monitoring and incident detection strategies.
- Respond: Ensures agencies follow appropriate incident response procedures.
- Recover: Evaluates the effectiveness of recovery plans and activities after an incident.

State and Local Incident Response Teams (CSIRT/IR Teams)

- Govern: Plays a role in the governance of incident response across the agency by adhering to established protocols and frameworks. Participates in the development and revision of governance policies related to incident handling, ensuring that response activities are standardized and comply with statewide requirements.
- 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

- Govern: Influences the governance of cybersecurity through the design and implementation of secure architectural solutions and systems. Engineers and architects contribute to the development of security standards and guidelines that govern system design and construction. Analysts participate in the governance process by providing insights into threat landscapes, contributing to the development of policies and procedures that guide protective measures and response strategies.
- 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.

1.5 Florida Digital Service (FLDS)

Following Governor Ron Desantis' call to modernize state government, the Florida Legislature created the Florida Digital Service (FLDS) in 2020 to develop and implement the state's enterprise-wide cybersecurity, data interoperability, and cloud-first initiatives. FLDS supports state agencies and local governments in strengthening cybersecurity, securing critical systems, and ensuring the resilience of Florida's public sector technology infrastructure.

FLDS manages Florida's first Cybersecurity Operations Center, facilitates data sharing between state agencies, and leverages the state's purchasing power to deliver taxpayer savings in technology procurement. Through collaboration with state agencies, local governments, and key stakeholders, FLDS works to enhance cybersecurity capabilities, improve risk management, and provide strategic guidance for securing Florida's digital assets.

Engagement with FLDS

State and local government entities are encouraged to actively engage with FLDS to access cybersecurity resources, training opportunities, and compliance support. FLDS facilitates regular meetings, webinars, and discussions to ensure cybersecurity leaders across Florida's public sector are informed and prepared to address emerging cyber threats.

FLDS remains committed to enhancing cybersecurity resilience statewide, ensuring that both state agencies and local governments have the tools, knowledge, and support needed to protect Florida's digital infrastructure.

To ensure continuity in communication with FLDS, especially during staffing changes, it is recommended to use a functional or distribution email address (e.g., cybersecurity@yourcounty.fl.gov) as the primary contact for your entity instead of individual staff email addresses.

1.6 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 https://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.

Office of Enterprise Technology: service@digital.fl.gov

The Office of Enterprise Technology is dedicated to overseeing the technical aspects of the state's IT strategy, covering Enterprise Architecture, Project Oversight, and Technology Assessment. Within this framework, the Enterprise Architecture team concentrates on crafting IT governance and the Enterprise Reference Architecture. The Program Management Office team provides project oversight and advisory support, collaborating closely with state agencies throughout the IT project lifecycle to ensure alignment with strategic goals and regulatory requirements.

General Inquiries: CIO@digital.fl.gov

This is the general inbox for the Chief Information Officer's office. If your inquiry doesn't fit into one of the more specialized categories, or if it's a higher-level concern that requires executive attention, this is the place to send it. This could range from strategy questions and vendor inquiries to governance issues.

Office of Administration and Policy:

- For questions related to **Policy, Florida Statute, or Rule**, contact policy@digital.fl.gov.
- For all **CoLab** related questions, contact CoLab@digital.fl.gov.

The Office of Administration and Policy oversees a wide range of administrative functions within the organization to provide smooth day-to-day operations. The office manages budget, procurement, contract management, purchasing requests, facilities management, human resources, professional development, communications, marketing, legislative policy compliance, and operational rules. This division ensures that the organization adheres to laws, policies, and statutes while fostering an environment of innovation and regulatory compliance.

1.7 Florida Cybersecurity Advisory Council

The Florida Cybersecurity Advisory Council was established under section 282.319, Florida Statutes, within the Florida Department of Management Services (DMS) to enhance the state's cybersecurity posture. The Council advises state leaders on cybersecurity risks, policies, and best practices, supporting both state agencies and local governments in strengthening their security programs. The Florida Cybersecurity Advisory Council collaborates with FLDS, federal agencies, private industry, and cybersecurity experts to improve cyber resilience, assess risks, and promote information sharing. The Council also works to identify cybersecurity challenges, particularly for critical infrastructure sectors and provides annual legislative recommendations to enhance Florida's cybersecurity framework. As a statutorily required body, the Council meets quarterly to review cybersecurity policies, assess risks, and develop strategic recommendations that align with national standards and industry best practices.

FLORIDA
CYBERSECURITY
ADVISORY COUNCIL

Section 2: Cybersecurity Training

2.1 Training Requirements

Cybersecurity training is a foundational component of protecting local government networks and data from cyber threats. Florida law requires all local government employees and technology professionals to complete cybersecurity training to strengthen awareness, reduce risks, and improve response capabilities.

Per Florida Statutes section 282.3185(3):

Basic Cybersecurity Training (Awareness)

The Florida Digital Service develops a basic cybersecurity training curriculum for local government employees to establish fundamental security knowledge.

Who Must Complete 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.

Purpose of Training:

- Increase awareness of cybersecurity risks.
- Educate employees on safe online practices to prevent cyberattacks.
- Reinforce best practices for password security, phishing prevention, and incident reporting.

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).

Who Must Complete Training?

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 help organizations reduce risk by ensuring employees understand cybersecurity threats and adopt best practices to prevent cyber incidents.

Cybersecurity Awareness

Cybersecurity awareness is a passive educational effort designed to keep cybersecurity at the forefront of employees' minds. It involves ongoing exposure to cybersecurity topics through:

- Posters, billboards, and flyers promoting security best practices.
- Newsletters and bulletins highlighting cyber threats and prevention tips.
- Broadcast advertisements or email reminders reinforcing safe behaviors.

Recommendations:

- Provide visual reminders (posters, flyers, and newsletters) to reinforce training and encourage cybersecurity awareness.
- Establish a centralized approach for distributing cybersecurity materials across departments.

Cybersecurity Awareness Training

Cybersecurity awareness training takes a more interactive approach by providing structured education to employees with network access. This ensures they recognize cyber threats and adopt secure behaviors in daily operations.

Curriculum for All Employees

- Initial Cybersecurity Awareness Training (First 30 Days)
- (New employees must complete this within their first 30 days)

Introduction to Cybersecurity Awareness

- Importance of cybersecurity in protecting data, systems, and public trust.
- Basic cybersecurity terminology and concepts.
- Employee roles and responsibilities in network security.

Recognizing Common Cyber Threats

- Phishing attacks and how to identify suspicious emails.
- Malware threats (viruses, ransomware, trojans).
- Social engineering techniques (impersonation, pretexting, baiting).

Password Security and Authentication

- Importance of strong passwords and multi-factor authentication (MFA).
- Secure password management (password managers, best practices).

Safe Web Browsing and Email Practices

- Identifying malicious websites and avoiding risky downloads.
- Safe email habits (checking senders, spotting fraudulent links).

Incident Reporting and Response

- How to report cybersecurity incidents (who to contact, process).
- Recognizing urgent vs. non-urgent security issues.

Annual Cybersecurity Awareness Training

- (Required for all employees annually; builds on initial training)

Refresher: Common Cyber Threats and Password Security

- New phishing techniques and real-world case studies.
- Password security updates (MFA, password manager usage).

Social Media and Online Privacy

- How cybercriminals exploit social media for attacks.
- Privacy settings and limiting personal data exposure.

Handling Sensitive Data Safely

- Proper storage and sharing of sensitive data.
- Recognizing classified vs. public data.
- Avoiding unauthorized cloud storage and email use for sensitive data.

Secure Use of Workplace Technology

- Understanding organization-approved apps and software.
- Risks of using personal devices for work-related activities.

2.3 Cybersecurity Role-Based Training

Cybersecurity role-based training ensures that individuals receive targeted education and skills development based on their job responsibilities. Local governments may have varying levels of cybersecurity expertise across their workforce, so it is essential to structure training in a way that is practical, manageable, and aligned with cybersecurity best practices.

This section categorizes role-based training into three main groups:

1. Cybersecurity Awareness Training for Non-Technical Roles (Executives and General Employees with Elevated Access)
2. Technical Cybersecurity Training for IT and Cybersecurity Personnel (System Administrators, Security Engineers, CSIRT Members)
3. Incident-Specific Training for CSIRT Members

For a comprehensive breakdown of cybersecurity personnel training, including required certifications and technical training pathways, refer to Appendix A.

Cybersecurity Awareness Training for Non-Technical Roles

These roles do not require a technical cybersecurity background but must have a fundamental understanding of cyber risks, compliance requirements, and their role in incident response.

Executives & Decision Makers

Executives and decision-makers set policies, allocate budgets, and oversee security strategies. They need to understand cyber risks and legal responsibilities to make informed decisions.

Training Topics:

- Cyber Risk Management - Assessing and mitigating cybersecurity risks.
- Incident Response and Crisis Management - Understanding their role in decision-making during cyber incidents.
- Regulatory Compliance – Ensuring alignment with Florida Statute Section 282.3185.
- Third-Party and Vendor Risk Management – Recognizing supply chain security threats.
- Business Continuity and Disaster Recovery – Planning for cyber resilience.

General Employees with Elevated Access

Employees with access to sensitive financial, legal, or personnel data are frequent targets of cyber-attacks.

Training Topics:

- Handling Sensitive Data Safely – Preventing accidental data exposure.
- Social Engineering and Phishing Awareness – Recognizing fraudulent emails and scams.
- Secure File Transfers and Email Encryption – Safeguarding information in transit.
- Understanding Access Control Policies – Properly managing permissions.
- Incident Reporting Protocols – Knowing when and how to escalate security issues.

Technical Cybersecurity Training for IT and Cybersecurity Personnel

These roles require specialized cybersecurity knowledge, technical training, and hands-on experience with cybersecurity tools and processes. IT and cybersecurity personnel, including IT directors, system and network administrators, database administrators, security engineers, cybersecurity analysts, forensic investigators, and CSIRT members, are responsible for configuring and maintaining IT systems, actively monitoring security threats, and responding to cyber incidents. Their training focuses on infrastructure security, system hardening, threat detection, and incident response to ensure the protection of local government assets.

Training Topics

For training requirements, including recommended certifications and technical training pathways for IT & Cybersecurity Personnel, see Appendix A.

Incident-Specific Training for CSIRT Members

Cybersecurity Incident Response Teams (CSIRTs) consist of both technical and non-technical personnel who play a role in responding to cyber incidents. Training for CSIRT members should be focused on their responsibilities during an incident rather than general cybersecurity concepts. Members may include IT staff, legal representatives, public relations personnel, HR professionals, and executive leadership.

An effective CSIRT is composed of both Cybersecurity Specialists and System Development and IT Personnel, who are tasked with monitoring systems, identifying and containing incidents.

CSIRT training should take place in addition to role-based training to ensure team members are prepared for their incident response roles and fully understand the organization’s Incident Response Plan (IRP). While role-based training provides foundational cybersecurity knowledge, CSIRT training ensures all members understand their specific responsibilities in handling cybersecurity incidents. Annual training is recommended, with updates to response plans and capabilities communicated throughout the year.

Training Topics

- Incident Handling & Response Protocols – Following established response procedures during an event.
- Communication & Coordination – Working with internal teams, external partners, and stakeholders.
- Forensic Evidence Preservation – Ensuring proper data collection and maintaining chain of custody.
- Regulatory & Compliance Considerations – Understanding legal requirements during incident response.
- Post-Incident Review & Lessons Learned – Conducting after-action reports and improving future response strategies.
- Familiarization with the Incident Response Plan – Understanding specific roles and responsibilities outlined in the organization's IRP to ensure a coordinated response.

Implementation for Local Governments

To support local governments in implementing cybersecurity role-based training, FLDS recommends:

- Assessing Workforce Needs – Identifying who falls into each role category.
- Establishing a Training Plan – Ensuring employees complete required training within 30 days of hire and renew training annually.
- Leveraging Free and Low-Cost Training – Using state-supported programs and online cybersecurity courses.
- Tracking and Documenting Training Completion – Maintaining training logs to ensure compliance with Florida law.

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 to prepare technical personnel for industry certifications, with exam vouchers included.

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

- 🔗 Cyber Florida at the University of South Florida
- 🔗 University of South Florida – Cybersecurity Awareness
- 🔗 University of South Florida – Executive Courses + Industry Certification Prep Courses
- 🔗 Florida International University – Executive Courses
- 🔗 University of West Florida – Certification Prep + Technical Courses

FLDS CoLab Events:

FLDS CoLab Events offer a diverse array of free professional training sessions specifically designed to cater to the needs of state and local government sectors. Some of these events are approved for ISC2 Continuing Professional Education (CPE) credits, while others are designed to meet Project Management Professional (PMP) Continuing Education Units (CEUs) or Professional Development Units (PDUs) requirements.

- ISC2 CPEs: Select events are geared towards those holding ISC2 certifications, allowing attendees to earn CPE credits to maintain their credentials.
- PMP Continuing Education: Other events focus on the continuing education requirements for Project Management Professionals, providing sessions that qualify for PMP CEUs or PDUs.
- Event Specifics: Each event will specify whether it qualifies for ISC2 CPEs or PMP Continuing Education credits.
- Remote Option: For those unable to attend in person, a remote participation option is available when possible, ensuring you can benefit from these specialized training sessions no matter what your location.

To receive updates on upcoming FLDS CoLab events and to find out which sessions qualify for ISC2 CPEs or PMP Continuing Education, subscribe to notifications by emailing CoLab@digital.fl.gov.

Other Free Training Opportunities:

For any additional questions or recommendations for inclusion in our 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 cybersecurity risks. Each local government must establish a risk-based approach to cybersecurity by adopting recognized security frameworks and best practices suited to its environment and risk profile.

While Florida law references the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) as an example of an industry best practice, local governments may choose to adopt alternative frameworks that align with their operational needs. Regardless of the framework, effective cybersecurity risk management includes:

- Identifying and mitigating risks to critical systems.
- Establishing and maintaining security policies and controls.
- Continuously monitoring systems for threats and vulnerabilities.
- Prioritizing cybersecurity investments to protect public sector services.

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.

Resource: The NIST Cybersecurity Framework (CSF) 2.0https://csf.tools/reference/nist-cybersecurity-framework/v1-1/

3.3 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 available to help organizations develop cybersecurity programs. While this handbook highlights the NIST Cybersecurity Framework as a widely accepted standard, local governments may choose a framework that best fits their operations, risk tolerance, and compliance requirements.

The NIST CSF is a flexible, risk-based approach to managing cybersecurity. Its key components include:

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

Govern: Align cybersecurity strategy, policies, and decision-making with business objectives.

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 six 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 framework provides informative references, such as industry standards, best practices, and guidelines, that organizations can use to support the implementation of the framework.

3.4 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.

The attestation should confirm:

- 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 incidents 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 (CSIRT) is a dedicated group of professionals within the organization responsible for managing and responding to cybersecurity incidents. The primary purpose of the CSIRT is to minimize the impact of security incidents, protect systems and data, and coordinate an effective recovery.

It is recommended that CSIRT members convene immediately upon notice of a Cybersecurity Incident. Best practices recommend the responsibilities of CSIRT members include:

- Convening a simple majority of CSIRT members at least quarterly to review, at a minimum, established processes and escalation protocols.
- Receiving incident response training annually.

The CSIRT 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:

1. Inform employees of their roles and responsibilities.
2. 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.
3. Share information, consistent with response plans.
4. Coordinate with Stakeholders, consistent with response plans.
5. 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 respond and support recovery activities adequately. Related activities may include:

- Each organization may establish notification thresholds and investigate notifications from detection systems.
- Each organization may assess and identify the impact of Incidents.
- Each organization may perform forensics, where deemed appropriate.
- Each organization may categorize incidents, consistent with response plans. Each Incident report and analysis, including findings and corrective actions, may be documented.
- 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.

4.3 Local Government Incident Reporting Process

IR.digital.fl.gov

Three Ways to Contact Us

- ir.digital.fl.gov – preferred method for incident reporting
- csoc@digital.fl.gov
- CSOC Phone: (850) 412-6074

Reporting to Law Enforcement

- The FLDS 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 FLDS 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 5: Legal and Regulatory Considerations

5.1 F.S. 119.0725 – Public Records Exemption

Pursuant to Florida Statutes section 119.0725, specific cybersecurity-related information held by government agencies is confidential and exempt from public records requests under s. 119.07(1) and s.24(a), Art. I of the State Constitution. These exemptions exist to protect sensitive data, critical infrastructure, and cybersecurity incident details from unauthorized disclosure that could compromise security and public safety.

Exempt Cybersecurity Information Includes:

1. **Insurance and Risk Mitigation Details:** Coverage limits, deductibles, and self-insurance details related to IT and operational technology protection.
2. **Critical Infrastructure Information:** Data concerning essential IT and operational technology systems.
3. **Cybersecurity Incidents:** Incident details reported under s. 282.318 or s.282.3185.
4. **Network and Security Configurations:** Schematics, encryption details, and detection or response strategies that could expose systems to cyber threats.

Exemptions for Cybersecurity Meetings:

- Any portion of a meeting that discusses exempt cybersecurity information is closed to the public and must be recorded and transcribed.
- The recording and transcript remain confidential under s. 119.07(1) and s. 24(a), Art. I of the State Constitution.

Who Can Access Exempt Information?

- Law enforcement agencies, the Auditor General, the Cybercrime Office of FDLE, and the Florida Digital Service (FLDS).
- Agencies may share confidential information with other government entities to fulfill official duties.

Additional Provisions:

Cybersecurity incident reports may be shared in aggregate form to protect sensitive details.

5.2 F.S. 112.22 – Use of applications from foreign countries of concern prohibited.

Pursuant to Florida Statutes section 112.22, Florida prohibits the use of certain applications on government issued devices to mitigate cybersecurity risks posed by foreign adversaries.

Definition of Prohibited Applications:

Applications that meet any of the following criteria:

- Created, maintained, or owned by a foreign principal from a foreign county of concern.
- Collect keystrokes or sensitive personal, financial, or proprietary data.
- Compromise email systems and act as vectors for ransomware deployment.
- Pose a security risk to government records, digital assets, or networks.

Public Employer Responsibilities:

- Block all prohibited applications from public access on any network or virtual private network that it owns, operates, or maintains.
- Restrict access to any prohibited application on a government-issued device.
- Ensure remote wipe and uninstallation of prohibited applications from any compromised government-issued device.
- Require employees to remove prohibited applications from their government-issued devices within 15 days of a list update.

Prohibited Applications List (Updated: April 22, 2025)

The Department of Management Services, through the Florida Digital Service, has determined the following applications meet the criteria for prohibited applications established in section 112.22(1)(f), Florida Statutes:

- QQ
- TikTok
- WeChat
- VKontakte
- Kaspersky
- Temu
- Tutor.com
- CamScanner
- SHAREit
- AliExpress
- DeepSeek
- Rednote
- Lemon8
- Xender
- Baidu Search
- Baidu Maps
- UC Browser
- WPS Office
- Moomoo
- Tiger Brokers
- VMate
- WeBull
- WeChat Pay
- CapCut

Waiver Process for Prohibited Applications

Public employers may request a waiver from the Department of Management Services (DMS) to allow designated employees or officers to use a prohibited application for law enforcement, cybersecurity research, or other critical functions.

Waiver Request Process:

1. Submit Form FLDS-02: Public employers must complete the Prohibited Application Waiver Request Form, available at Reference Material Home - Florida Administrative Rules, Law, Code, Register - FAC, FAR, eRulemaking.
2. Timeline Considerations:
   - Requests submitted within 5 days of a list update will be processed within 10 days.
   - Requests submitted outside of this timeframe will be processed within 30 days.
3. Evaluation Criteria:
   - The waiver must serve a recognized state interest such as public safety, law enforcement, or cybersecurity research.
   - A risk mitigation plan must be included to protect government systems, networks, and sensitive data.
4. Waiver Extensions:
   - Waivers are granted for up to 1 year.
   - Extensions must be requested at least 60 days before expiration.

Prohibited Applications List: Prohibited Applications List - Florida Department of Management Services

For waiver requests or inquiries, email: policy@digital.fl.gov

Section A: Appendix

A.1 Cybersecurity Work Roles and Recommended Role Based Training

This appendix provides an overview of recommended training and certification pathways for cybersecurity personnel. The roles and responsibilities outlined align with the National Initiative for Cybersecurity Education (NICE) framework and emphasize skill development through structured training, certifications, and hands-on experience.

Workforce Categories	Positions	Brief Position Description	Qualifications & Minimum Certification Requirements	Recommended Certifications for Advancement	Advanced Expertise & Strategic Leadership Certifications	Training Sustainment Methods
Oversee & Govern	Chief Information Security Officer (CISO)	The CISO is responsible for developing and leading an organization's cybersecurity strategy, policies, and risk management efforts. This role ensures alignment with business needs, oversees incident and threat response coordination, maintains regulatory compliance, and governs the overall security program. NICE Work Role Codes: OV-EXL-001 (Executive Cyber Leadership), OV-SPM-001 (Cybersecurity Program Manager), OV-LGA-002 (Authorizing Official)	• Bachelor's degree in Cybersecurity, Information Technology, Computer Science, or a related field (or equivalent work experience). • Minimum 7 years of experience in cybersecurity leadership roles. • Strong knowledge of cyber risk management and mitigation, security governance and regulatory compliance (e.g., NIST CSF, ISO 27001, HIPAA), enterprise security architecture, and executive communication and business alignment. • At least one of the following certifications: ○ Certified Information Security System Professional (CISSP) ○ Certified Information Security Manager (CISM) ○ Certified in Risk and Information Systems Control (CRISC) Note: A higher-level certification from the Recommended Certifications for Advancement or Advanced Expertise and Strategic Leadership categories may be substituted for the minimum certification requirement.	• CISSP - Information Systems Security Management Professional (CISSP-ISSMP) • CISSP – Information Systems Security Architecture Professional (CISSP-ISSAP) • CISSP – Information Systems Security Engineer Professional (CISSP-ISSEP) • Certified Chief Information Security Officer (CCISO) • GIAC Security Operations Certified (GSOC) • GIAC Cyber Threat Intelligence (GCTI) • GIAC Strategic Planning, Policy, and Leadership (GSTRT)	• Harvard Cybersecurity Leadership Certificate (or similar executive programs from SANS, MIT, Sanford, etc.) • NACD Cyber-Risk Oversight Certificate (for public sector and board engagement)	To maintain expertise and ensure continuous professional development, Chief Information Security Officers should: • Complete 40 hours of continuing education annually. • Participate in executive cybersecurity leadership training. • Engage in annual incident response exercises. • Stay current through cybersecurity conferences, summits, and workshops. • Maintain active involvement in cybersecurity operations, policy discussions, and governance initiatives.

Oversee & Govern	Information Security Manager (ISM)	The ISM oversees the implementation and execution of an organization's cybersecurity program. ISMs manage security operations, enforce policies, lead risk governance, and ensure compliance with regulatory frameworks to mitigate cyber risks. NICE Work Roles Codes: OV-MGT-001 (Cybersecurity Manager), OV-PMA-001 (IT Project Manager), OV-SPM-002 (Cybersecurity Program Manager)	• Bachelor's degree in Cybersecurity, Information Technology, Computer Science, or a related field (or equivalent work experience). • Minimum 5 years of experience in cybersecurity, risk management, or IT security leadership. • Strong understanding of risk management, regulatory compliance, security frameworks, security policy enforcement, and incident response coordination. • At least one of the following certifications: o Certified Information Systems Security Professional (CISSP) o Certified Information Security Manager (CISM) o Certified in Risk and Information Systems Control (CRISC) Note: A higher-level certification from the Recommended Certifications for Advancement or Advanced Expertise and Strategic Leadership categories may be substituted for the minimum certification requirement.	• Certified Information Systems Auditor (CISA) • GIAC Security Leadership Certification (GSLC) • Certified Information Privacy Manager (CIPM) • NIST Cybersecurity Framework Certification (NCFP) • GIAC Certified Incident Handler (GCIH)	• Harvard Cybersecurity Leadership Certificate (or equivalent program from SANS, Stanford, MIT) • NACD Cyber-Risk Oversight Certificate (for aligning with board-level governance and public sector engagement)	To maintain expertise and ensure continuous professional development, Information Security Managers should: • Complete 40 hours of continuing education annually. • Regularly participate in regulatory compliance and risk management training. • Engage in cybersecurity policy development initiatives. • Attend hands-on workshops to implement evolving frameworks and best practices. • Stay current through cybersecurity conferences and summits.
Oversee & Govern	Governance, Risk, and Compliance (GRC) Manager	The GRC Manager is responsible for developing, implementing, and managing an organization's cybersecurity governance, risk, and compliance programs. This role ensures adherence to cybersecurity policies, regulatory mandates, and industry best practices. NICE Work Role Codes: OV-GOV-001 (Cybersecurity Compliance Manager), OV-LGA-001 (Legal Advisor),	• Bachelor's degree in Cybersecurity, Information Technology, Risk Management, Business Administration, or a related field (or equivalent work experience). • Minimum 5 years of experience in: o Cybersecurity compliance, risk management, regulatory frameworks, or security governance. • Familiarity with frameworks such as NIST CSF, NIST 800-53, ISO 27001, and COBIT. • Understanding of compliance requirements (e.g., GDPR, HIPAA, FISMA, CMMC).	• Certified Information Security Manager (CISM) • Certified in the Governance of Enterprise IT (CGEIT) • Certified Data Privacy Solutions Engineer (CDPSE)	• CISSP - Information Systems Security Management Professional (CISSP-ISSMP) • GIAC Strategic Planning, Policy, and Leadership (GSTRT) • Certified Chief Information Security Officer (CCISO) • NACD Cyber-Risk Oversight Certificate	To maintain expertise and ensure continuous professional development, Governance, Risk, and Compliance Managers should: • Complete 40 hours of continuing education annually. • Attend cybersecurity governance and risk management workshops that focus on compliance updates, risk mitigation, and best practices. • Engage in compliance training and regulatory updates. • Collaborate with audit and risk teams to conduct security evaluations, risk assessments, and compliance audits. • Participate in cybersecurity summits, regulatory compliance forums, and professional associations.

		OV-RSK-001 (Risk Management Specialist)	• At least one of the following certifications: ○ Certified Information Systems Auditor (CISA) ○ Certified in Risk and Information Systems Control (CRISC) ○ CompTIA Security+ Note: A higher-level certification from the Recommended Certifications for Advancement or Advanced Expertise and Strategic Leadership categories may be substituted for the minimum certification requirement.			
Oversee & Govern	Cyber Policy and Strategy Planner	The Cyber Policy and Strategy Planner develops and maintains cybersecurity plans, policies, and strategies to support and align with enterprise cybersecurity initiatives and regulatory compliance. This role ensures adherence to legal and governance requirements, collaborates with business stakeholders, and aligns cybersecurity policy with organizational mission and risk posture. NICE Work Role Codes: OV-POL-001 (Cyber Policy and Strategy Planner), OV-MGT-001 (Cybersecurity Manager), OV-LGA-002 (Authorizing Official)	• Bachelor's degree in Public Policy, Cybersecurity, Information Technology, Law, or a related field (or equivalent work experience). • Minimum 5 years of experience in: ○ Cybersecurity policy development. ○ Governance, risk, and compliance. ○ Legal/ regulatory analysis related to cybersecurity. • Strong understanding of cybersecurity frameworks and regulatory mandates: ○ NIST CSF, NIST 800-53, ISO 27001, COBIT ○ GDPR, HIPAA, FISMA, CMMC • At least one of the following certifications: ○ CompTIA Security+ Note: A higher-level certification from the Recommended Certifications for Advancement or Advanced Expertise and Strategic Leadership categories may be substituted for the minimum certification requirement.	• Certified Information Security Manager (CISM) • Certified in Risk and Information Systems Control (CRISC) • Certified in the Governance of Enterprise IT (CGEIT)	• CISSP – Information Systems Security Management Professional (CISSP-ISSMP) • NACD Cyber-Risk Oversight Certificate • SANS Executive Cybersecurity Programs (Harvard, Stanford, or similar policy leadership programs)	To maintain expertise and ensure continuous professional development, Cyber Policy and Strategy Planners should: • Complete 40 hours of continuing education annually. • Participate in training on cybersecurity governance and policy development, risk frameworks and regulatory updates, and privacy, legal, and compliance standards. • Engage in legal and policy-focused cybersecurity workshops and conferences.

Oversee & Govern	Cyber Workforce Developer and Manager	The Cyber Workforce Develop and Manager is responsible for developing, implementing, and managing cybersecurity training programs to enhance workforce capabilities across an organization. This role ensures compliance with statutory training requirements, supports cybersecurity awareness initiatives, and fosters technical skill development aligned with the NICE Framework. NICE Work Role Codes: OV-TRN-001 (Cyber Instructional Curriculum Developer), OV-TRN-002 (Cyber Instructor), OV-MGT-001 (Cybersecurity Manager)	• Associate's degree in Cybersecurity, Information Technology, Workforce Development, or a related field (or equivalent work experience). • Minimum 5 years of experience in: o Cybersecurity training or workforce development. o Program or instructional leadership. o Exposure to NIST 800-50 and the NICE Framework. • Strong knowledge of: o Statutory training mandates (e.g., F.S. 282.318, NIST SP 800-50) o Competency-based learning frameworks. o Training needs analysis and program design. • At least one of the following certifications: o GIAC Security Essentials Certification (GSEC) o CompTIA Security+ Note: A higher-level certification from the Recommended Certifications for Advancement or Advanced Expertise and Strategic Leadership categories may be substituted for the minimum certification requirement.	• GIAC Strategic Planning, Policy, and Leadership (GSTRT) • Certified Information Security Manager (CISM) • Certified Technical Trainer (CTT+)	• GIAC Security Leadership (GSLC) • Certified Information Security System Professional (CISSP)	To maintain expertise and ensure continuous professional development, Cyber Workforce Developer and Managers should: • Complete 40 hours of continuing education annually. • Attend cybersecurity workforce development summits and training leadership forums. • Engage in state and federal cybersecurity workforce initiatives. • Collaborate with peers and leadership to align education strategy with cybersecurity risks and trends.
Oversee & Govern	Business Process Analyst	The Business Process Analyst is responsible for analyzing, documenting, and optimizing business processes to enhance cybersecurity operations and compliance. This role focuses on identifying efficiencies, automating workflows, and aligning operations with governance frameworks and organizational goals.	• Bachelor's degree in Business Administration, Cybersecurity, Information Systems, or a related field (or equivalent work experience). • Minimum 3 years of experience in: o Business process analysis. o Cybersecurity operations. o IT governance or workflow automation. • Proficient in:	• Certified Information Systems Auditor (CISA) • Certified in Risk and Information Systems Control (CRISC) • Lean Six Sigma Green Belt or Black Belt • Certified Data Privacy Solutions Engineer (CDPSE)	• Certified in the Governance of Enterprise IT (CGEIT) • Certified Information Security System Professional (CISSP) • GIAC Strategic Planning, Policy, and Leadership (GSTRT)	To maintain expertise and ensure continuous professional development, Business Process Analysts should: • Complete 40 hours of continuing education annually. • Participate in training on cybersecurity workflow automation, business process improvement, and risk mitigation strategies. • Engage in conferences and summits focused on cybersecurity governance, optimization tools, and process analysis best practices.

		NICE Work Role Codes: OV-BGA-001 (Budget and Acquisition Analyst), OV-GOV-001 (Cybersecurity Compliance Manager), OM-ANA-001 (Cybersecurity Analyst)	o Streamlining workflows for risk reduction and compliance. o Control implementation, process measurement, and cybersecurity documentation. o Business process modeling using tools like Business Process Model and Notation (BPMN) or Robotic Process Automation (RPA) technologies. • At least one of the following certifications: o CompTIA Security+ o ITIL Foundation o Certified Business Analysis Professional (CBAP) o PMI Professional in Business Analysis (PMI-PBA) Note: A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.		• CISSP – Information Systems Security Management Professional (CISSP-ISSMP)	
Investigate	Network Forensics Analyst	The Network Forensics Analyst is responsible for identifying, collecting, and analyzing network traffic and logs to investigate cyber incidents, detect intrusions, and support threat intelligence efforts. This role requires advanced expertise in packet analysis, malware reverse engineering, and intrusion detection to ensure accurate incident reconstruction and effective threat mitigation. NICE Work Role Code: IN-FOR-001 (Network Forensics Analyst)	• Bachelor's degree in Cybersecurity, Computer Science, Digital Forensics, or a related field (or equivalent work experience). • Minimum 3 years of experience in: o Network security, digital forensics, or incident response. o Packet analysis, log analysis, or threat intelligence operations. • At least one of the following certifications: o CompTIA Security+ (baseline cybersecurity competency) o Cisco Certified Network Associate (CCNA) (core networking knowledge critical for packet-level forensics)	• GIAC Certified Intrusion Analyst (GCIA) • GIAC Network Forensic Analyst (GNFA) • CompTIA CySA+ • GIAC Certified Incident Handler (GCIH) • ITIL Foundation	• GIAC Reverse Engineering Malware (GREM) • Certified Information Systems Security Professional (CISSP) • GIAC Certified Forensic Analyst (GCFA)	To maintain expertise and ensure continuous professional development, Network Forensics Analysts should: • Complete 40 hours of continuing education annually. • Participate in live incident response and forensic investigations. • Engage in hands-on labs focused on packet analysis, intrusion detection, and malware reverse engineering. • Join cyber threat intelligence and forensic security conferences. • Participate in Capture the Flag (CTF) exercises and cyber range simulations.

			o CompTIA Network+ (useful for fundamentals) Note: A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Investigate	Host Forensics Analyst	The Host Forensics Analyst is responsible for conducting forensic investigations on endpoints, servers, and storage devices to identify cyber incidents, reconstruct attack timelines, and support legal or compliance investigations. This role involves acquiring, preserving, and analyzing digital evidence while ensuring adherence to chain-of-custody protocols and forensic best practices. NICE Work Role Code: IN-FOR-002 (Host Forensics Analyst)	• Bachelor's degree in Digital Forensics, Cybersecurity, Computer Science, or a related field (or equivalent work experience). • Minimum 3 years of experience in: o Digital evidence acquisition and preservation. o Endpoint forensics, disk imaging, or file system analysis. • Expertise in: o Volatile memory analysis and malware reverse engineering. o Chain-of-custody documentation and forensic tool usage. o Endpoint and mobile forensics. • At least one of the following certifications: o CompTIA Security+ o CompTIA CySA+ o CompTIA Linux+	• GIAC Certified Forensic Examiner (GCFE) • GIAC Certified Forensic Analyst (GCFA) • GIAC Certified Incident Handler (GCIH) • EnCase Certified Examiner (EnCE) • AccessData Certified Examiner (ACE)	• Certified Information Systems Security Professional (CISSP) • GIAC Advanced Smartphone Forensics (GASF) • Certified Forensics Security Responder (CFSR)	To maintain expertise and ensure continuous professional development, Host Forensics Analysts should: • Complete 40 hours of continuing education annually. • Gain real-world experience through live forensic investigations or case-based simulations. • Engage in hands-on labs for disk imaging, memory forensics, and endpoint analysis. • Attend forensic and cybercrime conferences to stay informed on emerging tools and trends. • Participate in cyber range exercises to apply forensic skills in simulated attack environments.
Investigate	Cloud Forensics Analyst	The Cloud Forensics Analyst specializes in investigating cybersecurity incidents in cloud environments. This role involves analyzing cloud logs, metadata, and storage artifacts to detect unauthorized activity, reconstruct attack timelines, and support legal or compliance investigations. Analysts must understand	• Bachelor's degree in Digital Forensics, Cybersecurity, Computer Science, Cloud Computing, or a related field (or equivalent work experience). • Minimum 3 years of experience in: o Forensic investigations. o Cloud security, or o Incident response in cloud-hosted or hybrid environments. • Proficiency in:	• GIAC Certified Forensic Analyst (GCFA) • GIAC Cloud Forensics Responder (GCFR) • GIAC Cloud Security Automation (GCSA) • GIAC Certified Incident Handler (GCIH)	• GIAC Reverse Engineering Malware (GREM) • CISSP with Cloud Security concentration • CISSP + CCSP • GIAC Cyber Threat Intelligence (GCTI)	To maintain expertise and ensure continuous professional development, Cloud Forensics Analysts should: • Complete 40 hours of continuing education annually. • Engage in cloud IR simulations and cyber range exercises focused on cloud attack scenarios. • Participate in labs using platform-specific forensic tools (AWS, Azure, GCP) • Stay current through cloud security and forensics conferences. • Participate in hands-on threat hunting and SIEM monitoring exercises to sharpen detection skills.

		platform-specific forensic methods, incident response processes, and multi-cloud monitoring systems. NICE Work Role Code: IN-FOR-003 (Cloud Forensics Analyst — aligned with IN-FOR-001, PR-IN-001)	o Forensic data collection from cloud logs, storage, and VMs. o Cloud monitoring tools and SIEM systems. o Platform-specific incident response procedures (AWS, Azure, GCP) • At least one of the following certifications: o CompTIA Security+ o GIAC Cloud Security Essentials (GCLD) o Certified Cloud Security Professional (CCSP) o AWS Certified Cloud Practitioner Note: A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.	• Azure Security Engineer Associate / AWS Security Specialty		
Analyze	Penetration Tester	A Penetration Tester is responsible for simulating cyberattacks to identify vulnerabilities in networks, applications, cloud environments, and physical security controls. This role conducts controlled security assessments to determine how an adversary could exploit weaknesses and provide recommendations to improve defenses.	• Associate's degree in Cybersecurity, Computer Science, Information Security, or a related field (or equivalent work experience). • Minimum 3 years of experience in penetration testing, vulnerability assessment, or red teaming. • Proficient in adversary simulation, exploit development, and reconnaissance techniques to assess security weaknesses. • Strong knowledge of scripting and automation for security and system administration. • Familiarity with penetration testing, security assessment, and network analysis tools used for threat detection and vulnerability assessments. • Experience conducting controlled security tests that mimic advanced persistent threats (APTs) to evaluate an organization's security posture.	• Offensive Security Web Expert (OSWE) • GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) • Certified Red Team Operator (CRTO) • Cloud Penetration Tester (GCPN)	• Offensive Security Certified Expert (OSCE) • GIAC Certified Incident Handler (GCIH) • Licensed Penetration Tester (LPT) • Certified Red Team Lead (CRTL)	To maintain expertise and ensure continuous professional development, Penetration Testers should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on emerging exploitation techniques. • Participate in red team/blue team exercises to refine offensive and defensive security skills. • Engage in hands-on training with new hacking tools and exploits to strengthen penetration testing techniques. • Attend penetration testing and offensive security conferences to stay informed on cutting edge attack methods. • Collaborate with incident response teams to refine security controls and mitigation strategies.

			• At least one of the following certifications: o Certified Ethical Hacker (CEH) o GIAC Penetration Tester (GPEN) o Offensive Security Certified Professional (OSCP) **Note:** A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Analyze	Malware Analyst	A Malware Analyst identifies, analyzes, and mitigates malware threats that impact an organization's cybersecurity posture. Malware Analysts play a crucial role in cybersecurity operations by dissecting threats to strengthen an organization's security framework.	• Bachelor's degree in Cybersecurity, Computer Science, Digital Forensics, or a related field (or equivalent work experience). • Minimum 3 years of experience in malware analysis, digital forensics, or reverse engineering. • Proficient in static and dynamic malware analysis, including sandboxing, debugging, and decompilation techniques. • Strong understanding of operating system internals, file systems, and malware persistence techniques across diverse computing environments. • Experience with reverse engineering, binary analysis, and debugging tools for malware analysis and security research. • Familiarity with threat detection techniques, including pattern-based rule creation, indicator of compromise development, and malware classification.	• GIAC Certified Forensic Analyst (GCFA) • GIAC Certified Incident Handler (GCIH)	• Offensive Security Exploitation Expert (OSEE) • Certified Information Systems Security Professional (CISSP)	To maintain expertise and ensure continuous professional development, Malware Analysts should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on new malware threats and analysis techniques. • Participate in malware analysis and reverse engineering workshops to refine forensic investigation skills. • Attend cyber threat intelligence briefings and forensics conferences to stay informed on emerging threats. • Engage in capture-the-flag competitions and malware hunting exercises to improve hands-on skills in identifying and mitigating real world malware threats.

			• Proficiency in scripting and automation for security and system administration tasks. • At least one of the following certifications: o GIAC Reverse Engineering Malware (GREM) o Certified Reverse Engineering Analyst (CREA) o Certified Malware Analyst (CMA) **Note:** A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Analyze	Threat Intelligence Analyst	A Threat Intelligence Analyst collects, analyzes, and interprets data on cyber threats, adversary tactics, and emerging attack trends. They transform raw intelligence into actional insights to help organizations anticipate, prevent, and respond to cyber threats.	• Bachelor's degree in Cybersecurity, Computer Science, Intelligence Studies, or a related field (or equivalent work experience). • Minimum 3 years of experience in threat intelligence, cybersecurity analysis, or digital forensics. • Proficiency in collecting, analyzing, and disseminating cyber threat intelligence to enhance security operations. • Strong understanding of adversary tactics, techniques, and procedures (TTPs) and structured threat modeling frameworks. • Experience working with threat intelligence platforms (TIPs) and applying intelligence to security workflows. • Ability to analyze indicators of compromise, attack patterns, and malware behaviors to support detection and response efforts. • Proficiency in scripting and automation for security analysis and intelligence enrichment.	• GIAC Certified Incident Handler (GCIH) • Certified Information Systems Security Professional (CISSP)	• Certified Information Security Manager (CISM) • Offensive Security Certified Professional (OSCP)	To maintain expertise and ensure continuous professional development, Threat Intelligence Analysts should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on cyber threat trends and intelligence methodologies. • Participate in threat intelligence forums and intelligence-sharing groups to collaborate with industry professionals. • Attend cyber threat intelligence summits and conferences to stay informed on the latest threat actor activities and mitigation strategies. • Engage in dark web research and cybercrime monitoring exercises to track adversary tactics and emerging attack methods.

			• At least one of the following certifications: ○ Certified Threat Intelligence Analyst (CTIA) ○ GIAC Cyber Threat Intelligence (GCTI) ○ CompTIA Cybersecurity Analyst (CySA+) **Note:** A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Collect & Operate	Cybersecurity Analyst	A Cybersecurity Analyst is responsible for analyzing cybersecurity policies and protocols, conducting audits and risk assessments, and monitoring security controls within an organization. This role involves assessing security technologies, detecting and investigating security breaches, researching emerging cybersecurity threats, and preparing detailed incident metrics and reports.	• Associate's degree in Cybersecurity, Computer Science, Information Technology, or a related field (or equivalent work experience). • Minimum 2 years of experience in security monitoring, risk assessments, or incident response. • Familiarity with Security Information and Event Management (SIEM) tools. • Basic understanding of network security, firewalls, intrusion detection/prevention systems, and endpoint security. • Ability to analyze security alerts and investigate incidents. • Knowledge of fundamental cybersecurity frameworks to guide security assessments. • At least one of the following certifications: ○ CompTIA Security+ ○ GIAC Security Essentials (GSEC) ○ Certified SOC Analyst (CSA)	• CompTIA Cybersecurity Analyst (CySA+) • GIAC Certified Incident Handler (GCIH) • Certified Information Systems Security Professional (CISSP)	• Certified Information Security Manager (CISM) • GIAC Certified Intrusion Analyst (GCIA) • Certified Information Systems Auditor (CISA)	To maintain expertise and ensure continuous professional development, Cyber Analysts should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on new security threats and best practices. • Participate in cyber range exercises, penetration testing, and security simulation drills to enhance practical skills. • Attend cybersecurity workshops, training sessions, and professional conferences to stay current with industry trends. • Stay updated with threat intelligence reports, security research, and emerging cyber threats to anticipate and respond to new attack techniques.

			Note: A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Collect & Operate	Systems Analyst	A Systems Analyst is responsible for analyzing, designing, and improving IT systems to support cybersecurity operations. This role involves assessing vulnerabilities, implementing security controls, optimizing system performance, and ensuring compliance with cybersecurity policies.	• Bachelor's degree in Information Technology, Cybersecurity, Computer Science, or a related field (or equivalent work experience). • Minimum 2 years of experience in IT system administration, cybersecurity, or network infrastructure. • Knowledge of operating systems, system architectures, and cloud environments. • Familiarity with enterprise security tools, SIEM platforms, and system hardening techniques. • Basic understanding of cybersecurity frameworks and IT service management. • At least one of the following certifications: o CompTIA Security + o CompTIA Linux+ o Microsoft Certified: Security, Compliance, and Identity Fundamentals **Note:** A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be	• GIAC Certified Windows Security Administrator (GCWN) • CompTIA Cybersecurity Analyst (CySA+) • AWS Certified Security • Microsoft Certified: Azure Security Engineer Associate	• (ISC)2 Certified Information Security Professional (CISSP) • GIAC Security Essentials (GSEC) • Certified Information Systems Auditor (CISA)	To maintain expertise and ensure continuous professional development, Systems Analysts should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on new security threats and best practices. • Engage in hands-on system security assessments, vulnerability scanning, and penetration testing. • Participating in cyber range exercises and security workshops. • Staying updated with emerging threats, cybersecurity best practices, and system security patches.

			substituted for the minimum certification requirement.			
Collect & Operate	Security Information and Event Management (SIEM) Engineer	A SIEM Engineer is responsible for designing, implementing, and managing SIEM solutions to monitor and analyze security events across an organization's IT infrastructure. This role plays a key part in detecting, investigating, and mitigating cybersecurity incidents, ensuring compliance with security policies, and optimizing security operations through log management, correlation rules, and automation.	• Bachelor's degree in Information Technology, Cybersecurity, Computer Science, or a related field (or equivalent work experience). • Minimum 2 years of experience in SIEM administration, security monitoring, or network security operations. • Expertise in configuring, managing, and optimizing SIEM platforms, ensuring effective log collection, event correlation, and threat detection. • Experience integrating and operationalizing cyber threat intelligence, including indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) within security monitoring workflows. • Strong knowledge of security log sources, network and endpoint telemetry, and anomaly detection methodologies. • Proficiency in log ingestion, rule creation, event correlation, and automation to enhance detection and response capabilities. • Understanding of security frameworks and compliance requirements (e.g., NIST CSF, CIS Controls, PCI DSS, HIPAA, ISO 27001) as they relate to security monitoring and data collection.	• GIAC Certified Intrusion Analyst (GCIA) • Certified Information Systems Auditor (CISA) • Vendor-specific certifications depending on the SIEM platform used.	• Certified Information Systems Security Professional (CISSP) • GIAC Security Operations Certified (GSOC) • Certified Information Security Manager (CISM)	To maintain expertise and ensure continuous professional development, Security Information and Event Management (SIEM) Engineers should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on SIEM capabilities and security trends. • Engage in hands-on experience with threat detection, log correlation, and security automation to improve SIEM efficiency. • Participate in cyber range exercises and SIEM threat-hunting simulations to refine investigative and analysis skills. • Keep up with emerging security threats, SIEM updates, and new log analysis techniques to adapt to evolving cybersecurity challenges.

			• Familiarity with security data enrichment techniques and advanced analytics to improve threat detection and forensic investigations. • At least one of the following certifications: o GIAC Security Essentials (GSEC) o CompTIA Cybersecurity Analyst (CySA+) o Vendor-specific certifications depending on the SIEM platform used. Note: A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Collect & Operate	Application Developer	Application Developers design, build, test, and maintain secure applications. This role integrates security best practices throughout the Software Development Lifecycle to protect applications from vulnerabilities and ensure compliance with security policies and frameworks.	• Bachelor's degree in Software Engineering, Cybersecurity, Computer Science, or a related field (or equivalent work experience). • Minimum 2 years of experience in software development, with a focus on secure coding practices and security frameworks. • Proficiency in one or more programming languages commonly used in software development and security focused applications. • Familiarity with version control systems, API security principles, and secure software architecture. • Understanding of secure development methodologies, including threat modeling, Secure Software Development Lifecycle (SDLC), and DevSecOps best practices.	• Certified Ethical Hacker (CEH) • GIAC Web Application Penetration Tester (GWAPT) • GIAC Secure Software Programmer (GSSP-Java, GSSP-NET, or GSSP-Python)	• Offensive Security Web Expert (OSWE) • Certified Secure Software Lifecycle Professional (CSSLP) • GIAC Defensible Security Architecture (GDSA)	To maintain expertise and ensure continuous professional development, Application Developers should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on secure coding standards and vulnerability management. • Participate in secure coding workshops to enhance practical knowledge of static and dynamic application security testing. • Engage in hands-on security testing exercise to practice web application security assessments and API security hardening. • Conduct ongoing research on emerging application security threats to stay ahead of zero-day vulnerabilities, new exploitation techniques, and evolving secure coding methodologies.

			• Knowledge of security standards and frameworks related to secure software development and application security. • At least one of the following certifications: ○ Certified Secure Software Lifecycle Professional (CSSLP) ○ GIAC Secure Software Programmer (GSSP) ○ Certified Ethical Hacker (CEH) **Note:** A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Protect & Defend	Cybersecurity Operations Coordinator	Cybersecurity Operations Coordinators oversee and coordinate cybersecurity operations within an organization, ensuring that defensive security measures align with policies, frameworks, and threat intelligence. This role serves as a central point for coordinating security monitoring, incident response, and cybersecurity governance functions.	• Bachelor's degree in Cybersecurity, Information Technology, Computer Science, or a related field (or equivalent work experience). • Minimum 3 years of experience in cybersecurity operations, security monitoring, or incident coordination. • Strong knowledge of security frameworks, adversary tactics, and operational best practices for proactive defense and threat mitigation. • Experience with security monitoring, log analysis, and event correlation to detect, investigate, and respond to cyber threats. • Ability to coordinate and orchestrate security responses, collaborate with SOC teams, and ensure adherence to cybersecurity policies and compliance requirements. • Familiarity with cyber threat intelligence sources, attack techniques, and emerging security threats to enhance defensive strategies.	• Certified SOC Analyst (CSA) • GIAC Certified Enterprise Defender (GCED) • Certified Incident Handler (GCIH) • Cybersecurity Analyst (CySA+)	• Certified Information Systems Security Professional (CISSP) • GIAC Security Leadership Certification (GSLC) • Certified Information Security Manager (CISM) • Certified Cyber Operations Professional (CCOP)	To maintain expertise and ensure continuous professional development, Cybersecurity Operations Coordinators should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on cybersecurity operations and defensive strategies. • Participate in incident response exercises and tabletop simulations to improve security coordination and decision-making. • Engage in hands-on training in threat intelligence and SOC operations to strengthen incident detection and analysis capabilities. • Join cybersecurity leadership forums and working groups to stay current on evolving cyber defense strategies and security operations best practices.

			• At least two of the following certifications: ○ CompTIA Security+ ○ CompTIA Network+ ○ GIAC Security Operations Certified (GSOC) ○ Certified Incident Handler (GCIH) ○ CompTIA Cloud+ ○ Cyber Network Defender (CND) Note: A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Protect & Defend	Security Information and Event Management (SIEM) Analyst	A SIEM Analyst is responsible for monitoring, analyzing, and responding to security events and incidents using SIEM platforms. This role ensures logs and security data from various sources are collected, correlated, and analyzed to detect potential cyber threats. SIEM Analysts work closely with security operations teams to enhance threat detection, response, and reporting.	• Associate's degree in Cybersecurity, Information Technology, Computer Science, or a related field (or equivalent work experience). • Minimum 2 years of experience in security monitoring, log analysis, or SIEM operations. • Proficiency in log collection, event correlation, and alert triage to detect and respond to security incidents. • Strong understanding of cyber threat indicators, adversary tactics, techniques, and procedures (TTPs). • Knowledge of network security, intrusion detection/prevention systems (IDS/IPS), and endpoint security solutions. • Familiarity with SOC operations, event escalation procedures, and security response playbooks. • Awareness of security frameworks and best practices related to logging, monitoring, and threat detection. • At least one of the following certifications:	• GIAC Security Operations Certified (GSOC) • Certified SOC Analyst (CSA) • GIAC Certified Detection Analyst (GCDA) • Cybersecurity Analyst (CySA+)	• Certified Information Systems Security Professional (CISSP) • GIAC Certified Enterprise Defender (GCED) • GIAC Security Leadership Certification (GSLC)	To maintain expertise and ensure continuous professional development, SIEM Analysts should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on security monitoring techniques. • Participate in SIEM platform training and workshops to improve log analysis, threat detection, and event correlation skills. • Engage in incident response exercises and SOC simulations to strengthen alert triage, investigation, and security escalation procedures. • Stay updated with threat intelligence and log analysis training to detect evolving cyber threats and improve SIEM detection rules.

			○ CompTIA Security+ ○ CompTIA Network+ ○ EC Council Cyber Network Defender (CND) **Note:** A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Protect & Defend	Senior Incident Responder	A Senior Incident Responder leads the detection, investigation, and mitigation of cybersecurity incidents. This role oversees incident response procedures, analyzes security events, and coordinates remediation efforts. The Senior Incident Responder is essential in ensuring rapid response to threats, minimizing impact, and improving security posture through lessons learned.	• Bachelor's degree in Cybersecurity, Information Technology, Computer Science, or a related field (or equivalent work experience). • Minimum 5 years of experience in incident response, digital forensics, or security operations. • Deep understanding of adversary tactics, techniques, and procedures (TTPs) and the use of threat intelligence for incident response. • Expertise in digital forensics, evidence collection, malware analysis, and forensic investigation techniques. • Proficiency in log analysis, security event correlation, and real-time incident detection. • Strong knowledge of incident response frameworks, security playbooks, and automated response mechanisms for threat containment and remediation. • Familiarity with security standards and frameworks related to incident response and cybersecurity resilience. • At least one of the following certifications: ○ CompTIA Cybersecurity Analyst (CySA+)	• GIAC Certified Forensic Analyst (GCFA) • Certified Threat Intelligence Analyst (CTIA) • GIAC Security Operations Certified (GSOC) • GIAC Certified Detection Analyst (GCDA)	• Certified Information Systems Security Professional (CISSP) • GIAC Security Leadership Certification (GSLC) • Certified Information Security Manager (CISM) • GIAC Certified Incident Manager (GCIM)	To maintain expertise and ensure continuous professional development, Senior Incident Responders should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on incident response methodologies. • Participate in red team/blue team cyber range exercises to enhance real-world threat detection and response skills. • Engage in hands-on incident response simulations and tabletop exercises to improve decision making during security incidents. • Pursue advanced malware analysis and forensic training to gain expertise in reverse engineering and threat intelligence. • Regularly participate in cyber threat intelligence briefings to stay ahead of emerging cyber threats and attack techniques.

			○ GIAC Certified Incident Handler (GCIH) ○ EC Council Certified Incident Handler (ECIH) Note: A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Protect & Defend	Incident Responder	An Incident Responder is responsible for detecting, analyzing, containing, and mitigating cybersecurity incidents. They work within a Security Operations Center or Incident Response Team to investigate security events, apply response procedures, and coordinate remediation efforts.	• Associate's degree in Cybersecurity, Information Technology, or a related field (or equivalent work experience). • Minimum 2 years of experience in incident response, security monitoring, or digital forensics. • Strong understanding of cyber threats, security event correlation, and intrusion detection methodologies. • Experience in log analysis, event detection, and security alert triage to support real-time incident investigation. • Knowledge of memory forensics, malware analysis, and proper handling of digital evidence. • Familiarity with secure response playbooks, containment strategies, and mitigation techniques for incident resolution. • Awareness of security frameworks and best practices related to incident response and cybersecurity resilience. • At least one of the following certifications: ○ CompTIA Security+ ○ CompTIA Cybersecurity Analyst (CySA+) ○ GIAC Certified Incident Handler (GCIH)	• EC Council Certified Incident Handler (ECIH) • GIAC Certified Forensic Analyst (GCFA) • Certified Threat Intelligence Analyst (CTIA) • GIAC Security Operations Certified (GSOC)	• Certified Information Systems Security Professional (CISSP) • GIAC Certified Incident Manager (GCIM) • Certified Information Security Manager (CISM) • GIAC Security Leadership Certification (GSLC)	To maintain expertise and ensure continuous professional development, Incident Responders should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on incident response methodologies. • Participate in hands-on incident response simulations and tabletop exercises to enhance incident handling, decision making, and coordination skills. • Engage in red team/blue team cyber range training to strengthen threat detection and response capabilities. • Pursue ongoing training in SIEM analysis and threat intelligence to improve security monitoring and proactive defense strategies. • Attend cybersecurity conferences and SOC analyst workshops to stay ahead of evolving cyber threats and security operations best practices.

			Note: A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Operate & Maintain	Helpdesk Technician	A Helpdesk Technician serves as the first point of contact for IT and cybersecurity-related support within an organization. This role provides technical assistance, troubleshoots hardware and software issues, and ensures that employees adhere to cybersecurity best practices. Helpdesk Technicians play a crucial role in securing IT systems, educating users on security risks, and managing access controls.	• Associate's degree in Cybersecurity, Information Technology, Computer Science, or a related field (or equivalent work experience). • Minimum 1 year of experience in IT support, system administration, or technical troubleshooting. • Ability to diagnose and resolve IT issues, manage user accounts, and enforce access controls. • Understanding of multi-factor authentication (MFA), role-based access control (RBAC), and password management best practices. • Knowledge of common cybersecurity threats, including phishing, malware, and social engineering tactics. • Experience with basic network troubleshooting, operating system configurations, and IT asset management. • Familiarity with security policies, safe browsing practices, and endpoint protection strategies. • At least two of the following certifications: o CompTIA IT Fundamentals+ (ITF+) o CompTIA A+ o Certified Service Desk Support Technician (CSDST) Note: A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and*	• CompTIA Network+ • HDI Support Center Analyst (HDI-SCA) • Certified Support Specialist (CSS) • Certified Identity and Access Manager (CIAM)	• CompTIA Security+ • Certified Endpoint Administrator (CEH-EA) • Certified Information Systems Security Professional (CISSP) • Certified Helpdesk Manager (CHDM)	To maintain expertise and ensure continuous professional development, Helpdesk Technicians should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on IT security best practices, troubleshooting methods, and security awareness training. • Participate in hands-on troubleshooting labs and IT support simulations to enhance technical problem-solving skills. • Engage in cybersecurity awareness training for IT support staff to improve phishing detection, password security, and identity management practices. • Pursue ongoing training in identity and access management security controls to strengthen user access security and privilege management. • Attend helpdesk technician workshops and IT support forums to stay informed about emerging IT service trends and security requirements.

			Strategic Leadership categories may be substituted for the minimum certification requirement.			
Operate & Maintain	Network Technician	A Network Technician is responsible for installing, maintain, and troubleshooting an organization's network infrastructure, ensuring secure and reliable connectivity. This role configures and supports network devices, monitors traffic for security threats, and assist in implementing cybersecurity policies related to network security.	• Associate's degree in Cybersecurity, Information Technology, Computer Science, or a related field (or equivalent work experience). • Minimum 2 years of experience in network administration, IT support, or cybersecurity operations. • Understanding of routers, switches, firewalls, wireless security, and network segmentation for secure network operations. • Knowledge of Access Control Lists (ACLs), firewall rule management, and network access policies to enhance security. • Familiarity with network analysis tools, intrusion detection/prevention systems, and security event logging to support proactive threat monitoring. • Experience with VPN configurations, secure remote access solutions, and encryption technologies for data protection.	• Certified Information Security Technician (CIST) • CompTIA Security+ • GIAC Certified Network Defender (GND) • System Security Certified Practitioner (SSCP)	• GIAC Certified Enterprise Defender (GCED) • Certified Information Systems Security Professional (CISSP) • GIAC Certified Intrusion Analyst (GCIA) • GIAC Security Leadership Certification (GSLC)	To maintain expertise and ensure continuous professional development, Network Technicians should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on network security best practices, troubleshooting methods, and security awareness training. • Participate in hands-on network security simulations and labs to enhance firewall configurations, VLAN management, and network segmentation skills. • Engage in cyber range exercises for network security to improve threat detection and incident response capabilities. • Pursue ongoing training in firewall management, intrusion detection, and VPN security to strengthen network protection measures. • Attend network security and cybersecurity conferences to stay informed about emerging threats, attack techniques, and best practices.

			• Awareness of NIST CSF, CIS Controls, and ISO 27001 network security best practices. • At least two of the following certifications: ○ CompTIA Network+ ○ Certified Network Defender (CND) ○ CompTIA A+ ○ Certified Information Security Technician (CIST) **Note:** A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Operate & Maintain	Network Administrator	A Network Administrator is responsible for maintaining, configuring, and securing an organization's network infrastructure, including firewalls, routers, switches, and wireless networks. This role ensures network reliability, availability, and security, monitor for potential threats, and apply updates to prevent vulnerabilities.	• Bachelor's degree in Networking, Cybersecurity, Information Technology, Computer Science, or a related field (or equivalent work experience). • Minimum 2 years of experience in network administration, IT support, or cybersecurity operations. • Expertise in LAN/WAN, VLANS, firewalls, and VPN configurations to ensure secure and efficient network operations. • Understanding of zero-trust architecture, multi-factor authentication (MFA), and access control policies for identity and access management. • Experience with threat detection, security logging, and intrusion prevention rules to enhance network defense. • Knowledge of network monitoring tools, packet analysis, and security event management for proactive security monitoring. • Familiarity with NIST CSF, CIS Controls, ISO 27001, and network security best	• CompTIA Security+ • System Security Certified Practitioner (SSCP) • GIAC Certified Enterprise Defender (GCED) • Certified Information Security Technician (CIST)	• Certified Information Systems Security Professional (CISSP) • GIAC Certified Intrusion Analyst (GCIA) • GIAC Security Leadership Certification (GSLC) • Certified Information Security Manager (CISM)	To maintain expertise and ensure continuous professional development, Network Technicians should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on network security best practices, troubleshooting methods, and security awareness training. • Participation in incident response and network security exercises to enhance threat detection firewall management, and access control enforcement. • Engage in cyber range exercises for network security to improve network hardening, segmentation, and secure configurations. • Stay updated on emerging network security threats and best practices through research, professional development programs, and industry training. • Attend network security and cybersecurity conferences to gain insights into threat intelligence, risk mitigation, and network security advancements.

			practices to ensure compliance and resilience. • At least two of the following certifications: ○ CompTIA Network+ ○ Certified Network Defender (CND) ○ CompTIA A+ ○ Certified Information Security Technician (CIST) **Note:** A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Operate & Maintain	System Administrator	A System Administrator is responsible for the installation, configuration, maintenance, and security of an organization's IT infrastructure, including servers, operating systems, cloud environments, virtualization platforms, and endpoint management solutions. This role ensures system reliability, security compliance, and operational efficiency while collaborating with IT and cybersecurity teams to mitigate risks, automate administrative tasks, and respond to security incidents.	• Bachelor's degree in Cybersecurity, Information Technology, Computer Science, or a related field (or equivalent work experience). • Minimum 2 years of experience in system administration, IT support, or cybersecurity. • Expertise in securing operating systems, managing security patches, and enforcing least privilege principles to reduce attack surfaces. • Knowledge of Linux/Windows server configurations, hypervisors, and cloud computing platforms for secure system operations. • Experience with endpoint detection and response (EDR), anti-malware solutions, and security event logging to enhance threat detection and response. • Understanding of multi-factor authentication (MFA), privileged access management (PAM), and identity governance for secure access control. • Familiarity with NIST CSF, CIS Controls, ISO 27001, and secure system	• CompTIA Network+ • CompTIA Server+ • Certified Information Systems Auditor (CISA)	• Certified Information Security Professional (CISSP) • GIAC Certified Enterprise Defender (GCED) • GIAC Security Leadership Certification (GSLC) • Certified Information Security Manager (CISM)	To maintain expertise and ensure continuous professional development, System Administrators should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on emerging threats, compliance requirements, and cybersecurity best practices. • Participate in incident response exercises to enhance threat detection, security monitoring, and system forensic investigation skills. • Engage in cybersecurity training for IT professionals to improve secure system configurations, cloud security, and automation practices. • Stay current with system security trends by researching threat intelligence reports, security advisories, and vulnerability assessments. • Attend IT and cybersecurity conferences and workshops to gain insights into advancements in infrastructure security and enterprise system management.

			administration best practices to ensure compliance and security resilience. • At least two of the following certifications: ○ CompTIA Security+ ○ Certified Network Defender (CND) ○ System Security Certified Practitioner (SSCP) ○ Certified Information Security Technician (CIST) **Note:** Higher-level certifications from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Operate & Maintain	Systems Analyst	A Systems Analyst plays a critical role in analyzing, designing, and implementing IT solutions that align with an organization's business and cybersecurity objectives. This role works closely with stakeholders, IT teams, and cybersecurity professionals to assess system requirements, improve efficiency, and ensure security best practices are integrated into system development and operations.	• Bachelor's degree in Cybersecurity, Information Technology, Computer Science, or a related field (or equivalent work experience). • Minimum 2 years of experience in IT systems analysis, business process improvement, or IT project coordination. • Understanding of IT workflows, data modeling, and process reengineering to enhance operational efficiency. • Familiarity with security assessment frameworks, compliance requirements, and risk analysis techniques to support secure IT operations. • Experience with identity governance, role-based access control (RBAC), and least privilege principles for secure access management. • Ability to evaluate IT solutions, optimize workflows, and integrate security controls into business operations for seamless security integration. • Awareness of NIST CSF, ISO 27001, CIS Controls, and ITIL security best practices	• Certified Information Systems Auditor (CISA) • ISACA Certified Information Security Manager (CISM) • Lean Six Sigma Green Belt (LSSGB) • GIAC Security Essentials Certification (GSEC)	• Certified Information Security Professional (CISSP) • ISACA Certified in Governance of Enterprise IT (CGEIT) • Project Management Professional (PMP) • Certified Risk and Information Systems Control (CRISC)	To maintain expertise and ensure continuous professional development, Systems Analysts should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated evolving system security risks, IT compliance requirements, and process improvement methodologies. • Participate in IT system security audits and compliance reviews to strengthen system governance, risk management, and regulatory alignment. • Engage in business process improvement workshops to optimize system efficiency, workflow automation, and cybersecurity best practices. • Attend IT governance and cybersecurity conferences and workshops to gain insights into emerging threats, security frameworks, and risk management strategies. • Stay updated on evolving system security risks and best practices through threat intelligence reports, security advisories, and professional development training.

			to ensure compliance and security alignment. • At least two of the following certifications: o CompTIA Security+ o Certified Business Analysis Professional (CBAP) o ITIL 4 Foundation o Certified Information Security Technician (CIST) o Certified Scrum Master (CSM) or PMI Agile Certified Practioner (PMI-ACP) Note: Higher-level certifications from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Operate & Maintain	Compliance Analyst	A Compliance Analyst ensures that an organization's IT and cybersecurity programs adhere to regulatory requirements, industry standards, and internal security policies. This role conducts compliance audits, risk assessments, and reporting activities to ensure adherence to frameworks such as NIST, HIPAA, CJIS, FISMA, and other relevant cybersecurity regulations. Compliance Analysts work closely with GRC teams, cybersecurity personnel, and legal departments to maintain an organization's risk and compliance posture.	• Bachelor's degree in Cybersecurity, Information Technology, Business Administration, or a related field (or equivalent work experience). • Minimum 2 years of experience in IT compliance, auditing, risk management, or governance. • Understanding of NIST CSF, ISO 27001, HIPAA, FISMA, and other regulatory frameworks to ensure compliance and risk mitigation. • Knowledge of compliance audits, security assessments, and risk management strategies to evaluate and strengthen security posture. • Experience in developing, enforcing, and maintaining IT security policies aligned with industry standards and organizational objectives. • Understanding of cybersecurity law, privacy regulations, and compliance best	• Certified Information Privacy Manager (CIPM) • Certified Information Security Manager (CISM) • Lean Six Sigma Green Belt (LSSGB) • Certified Compliance and Ethics Professional (CCEP)	• Information System Security Professional (CISSP) • Project Management Professional (PMP) • Certified Government Chief Information Officer (CGCIO) • Certified Third-Party Risk Professional (CTPRP)	To maintain expertise and ensure continuous professional development, Compliance Analysts should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated evolving cybersecurity regulations, risk management methodologies, and compliance best practices. • Engage in IT governance and compliance audit to enhance policy enforcement, risk assessment capabilities, and regulatory compliance. • Participate in cybersecurity policy and risk management conferences to gain insights into emerging compliance trends and cybersecurity governance. • Monitor evolving cybersecurity compliance requirements to ensure alignment with regulatory changes, industry standards, and legal mandates. • Pursue ongoing training in cybersecurity frameworks such as NIST, ISO 27001, and CMMC to improve audit readiness, compliance effectiveness, and risk mitigation strategies.

			practices to support regulatory adherence. • Awareness of NIST 800-53, CMMC, CJIS, and other compliance frameworks to enhance governance and security oversight. • At least one of the following certifications: o CompTIA Security+ o Certified in Governance, Risk, and Compliance (CGRC) o Certified Information Privacy Professional (CIPP) o Certified Information Security Auditor (CISA) o Certified Information Security Technician (CIST) Note: A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Operate & Maintain	Vulnerability Assessment Analyst	A Vulnerability Assessment Analyst is responsible for identifying, analyzing, and reporting security vulnerabilities in an organization's networks, systems, and applications. This role supports proactive risk mitigation by using tools such as vulnerability scanners, configuration assessment tools, and penetration testing frameworks to assess security gaps and compliance with industry best practices.	• Associate's degree in Cybersecurity, Information Technology, Computer Science, or a related field (or equivalent work experience). • A minimum of one year of experience in vulnerability management, cybersecurity assessments, or IT security operations. • Understanding of Common Vulnerabilities and Exposures (CVEs), vulnerability databases, and risk impact analysis. • Experience in securing system configurations, remediating vulnerabilities, and managing security updates.	• GIAC Certified Incident Handler (GCIH) • Certified Information Systems Auditor (CISA) • Certified Information Security Manager (CISM) • CompTIA Cybersecurity Analyst (CySA+)	• Offensive Security Certified Professional (OSCP) • (ISC)2 Certified Information Security Professional (CISSP) • GIAC Security Leadership Certification (GSLC) • Certified Risk and Information Systems Control (CRISC)	To maintain expertise and ensure continuous professional development, Vulnerability Analysts should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on emerging vulnerability trends, security threats, and best practices. • Regularly participate in vulnerability management programs to strengthen risk identification, security patching, and assessment methodologies. • Gain hands on experience with vulnerability assessment tools to improve network security scanning, system hardening, and risk mitigation techniques. • Continuously monitor Common Vulnerabilities and Exposures (CVEs) and emerging cybersecurity threats through intelligence feeds, security advisories, and research reports. • Engage in penetration testing labs and ethical hacking simulations to develop advanced security assessment skills, attack vector analysis, and defensive countermeasures.

			• Knowledge of attack vectors, threat modeling, and vulnerability exploitation techniques. • Familiarity with penetration testing frameworks, ethical hacking methodologies, and security assessment tools. • Awareness of NIST 800-53, CIS Controls, and ISO 27001 security guidelines. • At least one of the following certifications: o GIAC Security Essentials (GSEC) o Certified Vulnerability Assessor (CVA) o Certified Information Security Technician (CIST) o CompTIA Network+ Note: A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Operate & Maintain	DevSecOps Engineer	A DevSecOps Engineer integrates security practices into the DevOps pipeline, ensuring that security is a key component of software development, deployment, and operations. This role works closely with developers, operations teams, and security professionals to implement automated security controls, conduct vulnerability assessments, and manage secure software development lifecycle practices.	• Bachelor's degree in Information Technology, Cybersecurity, Computer Science, Software Engineering, or a related field (or equivalent work experience). • Minimum 2 years of experience in DevOps, Cloud Security, Application Security, or Secure Software Development. • Understanding of CI/CD pipelines, security automation, and Infrastructure as Code (IaC) to integrate security into DevOps workflows. • Knowledge of static and dynamic application security testing (SAST/DAST) and software composition analysis (SCA) for secure software development.	• Certified Kubernetes Security Specialist (CKS) • Certified Risk and Information Systems Control (CRISC) • Certified DevSecOps Professional (CDP) • Certified Information Systems Security Professional (CISSP)	• GIAC Security Leadership Certification (GSLC) • Certified Cloud Security Professional (CCSP) • Certified Secure Software Lifecycle Professional (CSSLP) • Certified Governance, Risk, and Compliance Professional (CGRCP)	To maintain expertise and ensure continuous professional development, DevSecOps Engineers should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on secure DevOps methodologies, software security trends, and automation techniques. • Participate in DevSecOps conferences and workshops to enhance secure software development knowledge and security integration skills. • Gain hands on labs in threat modeling, secure coding, and penetration testing through real-world simulations and security labs. • Engage in open-source security projects and security automation research to develop innovative security solutions and best practices. • Regularly review compliance standards and security policies to ensure alignment with NIST, ISO 27001, and secure SDLC requirements.

			• Experience in securing cloud-native applications, Kubernetes, and container security best practices to protect cloud environments. • Familiarity with identifying security threats, vulnerability scanning, and applying compliance frameworks to minimize security risks. • Awareness of secure SDLC principles, regulatory requirements, and security frameworks (e.g., NIST 800-53, ISO 27001) to ensure compliance and risk mitigation. • At least one of the following certifications: o GIAC Cloud Security Automation (GCSA) o Certified Secure Software Lifecycle Professional (CSSLP) o Certified Information Security Technician (CIST) o GIAC Defensible Security Architecture (GDSA) **Note:** A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.			
Securely Provision	System Administrator	A System Administrator in Securely Provision is responsible for configuring, managing, and maintaining IT systems and infrastructure with a focus on security. This role ensures that hardware, software, and networks are securely provisioned, deployed, and maintained in compliance with	• Bachelor's degree in Information Technology, Cybersecurity, Computer Science, or a related field (or equivalent work experience). • Minimum 2 years of experience in system administration, network administration, or IT support. • Understanding of Windows, Linux, and macOS security hardening techniques to protect system integrity.	• Certified Information Security Manager (CISM) • GIAC Security Leadership Certification (GSLC) • Certified Kubernetes Administrator (CKA) • GIAC Certified Windows Security Administrator (GCWN)	• Certified Information Security Professional (CISSP) • Certified Government Chief Information Officer (CGCIO) • Certified Risk and Information Systems Control (CRISC)	To maintain expertise and ensure continuous professional development, System Administrators should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on infrastructure security best practices, access control methodologies, and system hardening techniques. • Gain hands on training with system security tools and hardening techniques through virtual labs, cyber range exercises, and real-world simulations. • Participate in vulnerability management and security operations exercises to enhance patch management effectiveness and system security enforcement.

		cybersecurity policies and best practices.	• Knowledge of virtualization platforms, cloud computing environments, and security best practices for secure infrastructure management. • Experience in applying security patches, enforcing security configurations, and managing system updates to reduce vulnerabilities. • Familiarity with Active Directory (AD), role-based access control (RBAC), and authentication mechanisms to enhance identity security. • Awareness of NIST 800-53, ISO 27001, and CIS benchmarks to align with industry standards. • At least one of the following certifications: o CompTIA Security+ o CompTIA Network+ o GIAC Certified Windows Security Administrator (GCWN) o Certified Information Security Technician (CIST) o Certified System Security Practioner (CSSP) **Note:** A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.		• Certified Enterprise Defender (GCED)	• Engage in cybersecurity forums, webinars, and industry events to collaborate with peers, learn from security experts, and stay informed on emerging security threats. • Regularly review compliance standards and security policies to ensure alignment with NIST CSF, ISO 27001, and regulatory security requirements.
Securely Provision	Application Architect	An Application Architect designs and oversees the development of secure, scalable, and high performing applications. This role ensures that software solutions align with security best practices, organizational needs, and industry standards.	• Bachelor's degree in Cybersecurity, Computer Science, Software Engineering, or a related field (or equivalent work experience). • Minimum 5 years of experience in software architecture, secure software development, or application security. • Expertise in designing secure applications, threat modeling, and	• Certified Information Systems Security Professional (CISSP) • Certified DevSecOps Professional (CDP) • Certified Kubernetes Security Specialist (CKS) • Certified Risk and Information Systems Control (CRISC)	• Certified Enterprise Architect (CEA) • GIAC Security Leadership Certification (GSLC) • Certified Cloud Security Professional (CCSP)	To maintain expertise and ensure continuous professional development, Application Architects should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on emerging software, security trends, secure coding methodologies, and architectural risk assessment strategies. • Participate in secure software development and threat modeling workshops to enhance software security integration skills.

			architectural risk assessment to mitigate security vulnerabilities. • Knowledge of secure coding standards, OWASP Top 10, and SDLC security best practices to enhance software security. • Experience in identifying security threats, integrating countermeasures, and performing risk assessments to strengthen application defenses. • Awareness of NIST software security guidelines, ISO 27034, and secure DevSecOps methodologies to ensure regulatory compliance and secure development practices. • At least one of the following certifications: o GIAC Secure Software Programmer (GSSP) o Certified Secure Software Lifecycle Professional (CSSLP) o Certified Information Security Technician (CIST) o GIAC Defensible Security Architecture (GDSA) o CompTIA Security+ **Note:** A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.		• Certified Governance, Risk, and Compliance Professional (CGRCP)	• Attend application security and cloud security conferences to collaborate with security architects, learn from industry experts, and stay informed on evolving security threats. • Engage in code reviews, red team exercises, and penetration testing scenarios to identify security vulnerabilities and strengthen application defenses. • Stay current with OWASP Top 10 vulnerabilities and NIST software security guidelines to ensure compliance with best practices and risk mitigation strategies.
Securely Provision	Application Developer	An Application Developer is responsible for designing, coding, testing, and deploying secure software solutions. This role integrates secure coding practices into the software development lifecycle (SDLC) and works closely with security architects, DevSecOps	• Bachelor's degree in Cybersecurity, Computer Science, Software Engineering, or a related field (or equivalent work experience). • Minimum 2 years of experience in software development and secure coding.	• Certified Threat Modeling Professional (CTMP) • Certified Kubernetes Security Specialist (CKS) • Certified DevSecOps Engineer (CDSE) • GIAC Web Application Penetration Tester (GWAPT)	• Certified Enterprise Architect (CEA) • Certified Information Systems Security Professional (CISSP) • GIAC Defensible Security Architecture (GDSA)	To maintain expertise and ensure continuous professional development, Application Developers should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on emerging software, security trends, secure coding methodologies, and software security governance strategies. • Participate in secure coding bootcamps and workshops to enhance secure development skills and threat modeling capabilities.

		teams, and IT administrators to minimize vulnerabilities.	• Understanding of secure coding methodologies, software risk assessment, and integrating security into SDLC. • Knowledge of secure design patterns, software attack vectors, and security countermeasures to reduce application vulnerabilities. • Experience with static and dynamic code analysis, penetration testing, and vulnerability assessment to identify and remediate security flaws. • Awareness of application security best practices and frameworks such as OWASP Top 10, SANS CWE Top 25, NIST Secure Software Development Framework (SSDF), and ISO 27034. • At least one of the following certifications: o Certified Secure Software Lifecycle Professional (CSSLP) o GIAC Secure Software Programmer (GSSP) o Certified Application Security Engineer (CASE) o Certified Software Security Tester (CSST) o CompTIA Security+ **Note:** A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.		• Certified Risk and Information Systems Control (CRISC)	• Attend cybersecurity and application security conferences to collaborate with secure software professionals, learn from security experts, and stay informed on evolving security threats. • Engage in code reviews, threat modeling, and penetration testing exercises to identify security vulnerabilities and improve secure coding practices. • Stay current with OWASP Top 10, SANS CWE Top 25, and NIST Secure Software Development guidelines to ensure compliance with best practices and risk mitigation strategies.
Securely Provision	Security Architect	A Security Architect is responsible for designing and implementing secure IT infrastructures that align with an organization's security policies, compliance requirements, and best practices. Security	• Bachelor's degree in Cybersecurity, Information Security, Computer Science, or a related field (or equivalent work experience). • Minimum 5 years of experience in cybersecurity architecture, network security, and security operations.	• Certified Cloud Security Professional (CCSP) • GIAC Enterprise Security Architect (GDSA) • Certified Secure Software Lifecycle Professional (CSSLP)	• Certified Information Systems Auditor (CISA) • Certified Chief Information Security Officer (CCISO)	To maintain expertise and ensure continuous professional development, Security Architects should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on emerging security architecture trends, advanced security design methodologies, and enterprise security governance strategies.

		Architects develop cybersecurity frameworks, risk mitigation strategies, and security roadmaps to protect against evolving threats.	• Understanding of zero-trust models, defense-in-depth strategies, and architectural security frameworks to design resilient security architectures. • Knowledge of encryption methodologies, identity and access management (IAM) frameworks, and authentication mechanisms to protect sensitive data. • Experience in designing secure networks, implementing security controls, and securing cloud environments to mitigate cyber threats. • Awareness of ISO 27001, NIST SP 800-160, and security risk assessment frameworks to ensure compliance and risk management best practices. • At least one of the following certifications: o Certified Information Systems Security Professional (CISSP) o GIAC Security Leadership Certification (GSLC) o Certified Information Security Manager (CISM) **Note:** A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.	• TOGAF 9 Certified	• GIAC Security Expert (GSE) • Certified Governance, Risk, and Compliance Professional (CGRCP)	• Participate in advanced cybersecurity architecture workshops to enhance enterprise security planning and risk mitigation skills. • Attend security leadership conferences and security governance summits to collaborate with industry leaders, learn from security strategists, and stay informed on evolving cyber threats. • Conduct security risk assessments and architecture review to evaluate enterprise security effectiveness and recommend security improvements. • Stay current with NIST SP 800-160, ISO 27001, and MITRE ATT&CK to ensure compliance with industry security frameworks and strategic security defense methodologies.

Securely Provision	Security Engineer	A Security Engineer is responsible for designing, implementing, and maintaining security solutions that protect an organization's IT infrastructure. This role involves developing security controls, conducting vulnerability assessments, managing security tools, and collaborating with IT teams to ensure systems are protected against cyber threats. Security Engineers focus on network security, endpoint protection, access control, cloud security, and secure system configuration.	• Bachelor's degree in Cybersecurity, Information Security, Computer Science, or a related field (or equivalent work experience). • Minimum 3 years of experience in cybersecurity engineering, system hardening, and threat detection. • Expertise in firewalls, intrusion detection/prevention systems (IDS/IPS), endpoint protection, and secure system configuration to safeguard IT environments. • Understanding of security design principles, access control models, and secure loud frameworks to implement robust security measures. • Experience with security monitoring, threat intelligence, and cyber threat hunting techniques to identify and mitigate security threats. • Awareness of NIST CSF, ISO 27001, CIS Controls, and secure development best practices to ensure regulatory compliance and risk mitigation. • At least one of the following certifications: ○ CompTIA Security+ ○ GIAC Security Essentials (GSEC) ○ Certified Ethical Hacker (CEH) **Note:** A higher-level certification from the *Recommended Certifications for Advancement* or *Advanced Expertise and Strategic Leadership* categories may be substituted for the minimum certification requirement.	• Certified Cloud Security Professional (CCSP) • GIAC Certified Incident Handler (GCIH) • GIAC Security Operations Certified (GSOC) • Certified Penetration Testing Engineer (CPTE)	• Offensive Security Certified Professional (OSCP) • GIAC Enterprise Security Architect (GDSA) • Certified Information Security Manager (CISM) • Certified Information Systems Security Professional (CISSP) • GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)	To maintain expertise and ensure continuous professional development, Security Engineers should: • Complete 40 hours of continuing education annually to maintain certifications and stay updated on emerging security trends, threat intelligence, and security automation strategies. • Participate in cybersecurity engineering workshops and hands on labs to enhance technical security expertise and cyber defense capabilities. • Attend cybersecurity conferences and industry summits to network with security experts, discuss emerging threats, and learn about new security technologies. • Conduct penetration testing and vulnerability scanning exercises to identify system weaknesses and improve security posture. • Stay updated with NIST SP 800-53, MITRE ATT&CK, and emerging security frameworks to ensure compliance with best practices and evolving security standards.

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 Flds Responsibility Breakdowns

Section	Subsection	Party Responsible	Responsibility
282.3185	(3)(a)1	FLDS	Develop a basic cybersecurity training curriculum for local government employees.
282.3185	(3)(a)2	FLDS	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)	FLDS	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)	FLDS	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.

Florida Digital

Florida Digital Service
2555 Shumard Oak Blvd • Tallahassee, FL 32399
www.digital.fl.gov

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/

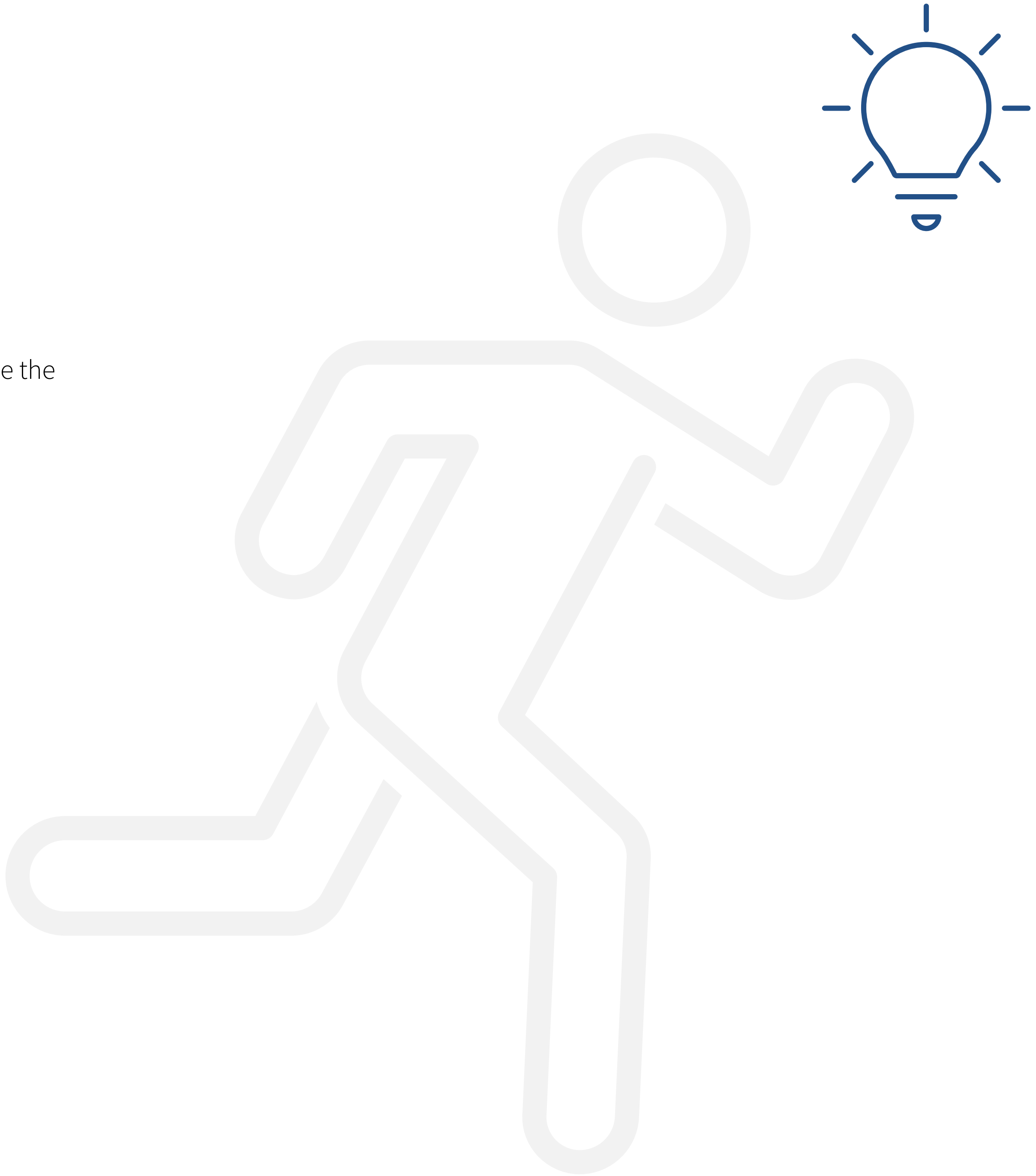
Florida Digital

Florida Digital Service
2555 Shumard Oak Blvd • Tallahassee, FL 32399
www.digital.fl.gov

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 FLDS will strive to provide full support.
    - ir.digital.fl.gov – preferred method for incident reporting
    - csoc@digital.fl.gov
    - CSOC Phone: (850) 412-6074

Florida Digital

Florida Digital Service
2555 Shumard Oak Blvd • Tallahassee, FL 32399
www.digital.fl.gov

A.6 Local Government Incident Reporting Process – Tear Out

IR.digital.fl.gov

Three Ways to Contact Us

- ir.digital.fl.gov – preferred method for incident reporting
- csoc@digital.fl.gov
- CSOC Phone: (850) 412-6074

Reporting to Law Enforcement

- The FLDS 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 FLDS 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).

Florida Digital

Florida Digital Service
2555 Shumard Oak Blvd • Tallahassee, FL 32399
www.digital.fl.gov