




EDUCATION | RESEARCH | OUTREACH

FMEA Briefing

Unclassified



This session will provide an in-depth overview of Cyber Florida's no-cost, state-funded cybersecurity services available to public and private sector organizations. Key topics include:

- Intelligence Update.
- Risk Mitigation Support
- Incident Preparedness and Response Counseling

Attendees will leave with clear steps on how to access these resources and integrate them into their organizational cybersecurity strategy



Cyber Florida Presenters

Bryan Langley and Emeka Okammor



The Cyber FL CIP Program offers no cost, AI-driven cybersecurity support tailored to Florida's critical infrastructure organizations, especially those who are resourced constrained.

Our program provides a single access point to tools aligned with the NIST Cybersecurity Framework 2.0, CIS Maturity Index, and Florida Statute 282.318—helping you strengthen your cyber posture and improve your assessment results.

Backed by the state, this program delivers real value when time, funding, and resources are limited.

Who Are We?

- **Established in 2014: FS 1004.444** Make Florida “the national leader in cybersecurity”
- **Education** Build/expand cybersecurity workforce development
- **Research** Enable/expand cybersecurity research capabilities across the state and enable technology innovation
- **Cybersecurity Public Policy** Shape public policy to enhance cybersecurity across the state.
- **Outreach** Public awareness campaigns and events to help vulnerable organizations enhance their cybersecurity
- **Events** Cyber Bay Conference, Cyber Launch, Podcasts “No Password Required”, Cyber Chat, & Video Blog.



Capacity-Building Engine

- Education + Workforce Development
- Research + Innovation
- Engagement + Collaboration
- Policy + Advocacy



RESEARCH
initiatives

Cyber Bay
Conference

Cyber
Florida
Studios





Security Operations Center Apprentice Program

Provides hands-on cyber threat monitoring, digital forensics, and reporting skills for up to 20 USF students each year

SERVICES OFFERED/STUDENT LEARNING OBJECTIVES

- Hands-on experience for students to bridge the gap between academia and work experience
- Students learn state-of-the-art real-time cybersecurity monitoring and threat detection tools
- Cybersecurity services include
 - Digital forensics, including enterprise and mobile devices
 - Incident response (remote triage assistance)
 - Malware analysis, Log management and review
 - Log collection and analysis
 - Cybersecurity projects, assessments, and consulting
 - Coming soon: vulnerability assessment and penetration, and testing



powered by **CYBER FLORIDA AT USF + SIMSPACE**



ALIGNED REALISTIC CYBERATTACK SIMULATION RANGE

RANGE FEATURES

- Florida County and Local government IT and OT cybersecurity personnel - public sector focused
- Cyber Range as a Service (CRaaS), 100% cloud-based training model
- No cost for public sector users
- Supports Statewide Training Program

KEY MILESTONES

- Launched March 2024: SimSpace selected as vendor; soft launch
- Currently 145 users across 17 counties on ARCS Range



CYBER FLORIDA FIRSTLINE

No-cost education & training
for Florida's public sector

\$30M in non-recurring funding from the Florida Legislature to provide no-cost cyber education and training to every Florida state, county, and municipal government employee

University of South Florida:

- 4- to 8-hour classes for executive, managerial, and general staff
- 4-week industry certification prep courses for technical roles
- A handbook for state and local government employees
- Mostly virtual (synchronous and asynchronous)

University of West Florida:

- 1- to 8-week industry certification prep courses for technical roles
- Mostly virtual (synchronous and asynchronous)

Florida International University:

- 8- to 16-hour classes for executive, managerial, and general staff
- FIU experience indicates in-person attendance is the most desired mode for this audience
- FIU partnered with 7 institutions across the state to minimize travel while providing more in-person sessions





- Grant-supported
- Industry partners include JPMorgan Chase, ReliaQuest, KnowBe4, Amazon Web Services, VMWare, Rapid7, Cisco, Raytheon, OPSWAT, GuidePoint

- **NICE Work Role:** Cyber Defence Analyst
- **Enrollment:** Two cohorts per year, 30-40 students per cohort
- **Courses/Badges:** Network Fundamentals, Cyber Defense Fundamentals
- **Industry Certifications:**
 - CompTIA Network+
 - CompTIA Cybersecurity Analyst (CySA+)
 - CompTIA Security+





- Youth Engagement
- Educator Professional Development
- Curriculum Development

PROGRAM HIGHLIGHTS

- Active in districts across Florida through a tiered support system, as well as several other states, territories, and even countries
- Cybersecurity Essentials Course (including lesson plans, presentations, labs, tests, and activities) preps for industry certification exam
- CyberHub virtual lab environment provided at no cost
- Speakers Bureau, monthly webinars, Slack channel w/150 users
- Collaboration Center housed in Canvas provides curriculum guides, demos, exam prep, career resources
- Second Annual CyberLaunch Statewide High School Competition 4 April 2025





- Over 1,000 high school students participating
- Career, Technical, and Education



PROGRAM HIGHLIGHTS

- Participated in a capture-the-flag competition from 47 school districts across Florida
- The CyberLaunch program aims to introduce high school students to the universe of cybersecurity careers through the fun of a statewide competition.
- The program includes resources for teachers and students who are new to cybersecurity, including classroom activities that provide a sneak peek of the competition platform for practice!
- Through this endeavor, we hope to build interest in cybersecurity careers, awareness of cybersecurity best practices, and help connect the cybersecurity industry in Florida with local school districts.



- No cost cyber risk assessment funded and authorized by the State of Florida
 - Entry-level assessment (20 questions) to identify vulnerabilities
 - Mid-level assessment (38 questions) measuring against the Cybersecurity Performance Goals (CPG)s
- Develop a Florida-Specific Cybersecurity Maturity Index/Model (MS-ISAC)
- Free resources for public and private sector critical infrastructure organizations, such as incident response plans, resource mapping, etc.
- Close the maturity gap for “basic” ransomware readiness
- Mapping tool (Cyber Bulls-i) to provide summaries for critical infrastructure cybersecurity initiatives using AI to map NIST 800-53 to all 106 CSF question
- Construct and maintain a comprehensive list of critical infrastructure entities operating in the state for sampling and communication purposes (intel sharing)





Florida Threat and Risk Landscape

Presenter: Bryan Langley



Nation-State Threat Actors

China



State-sponsored actors have infiltrated critical infrastructure, pre-positioning for potential attacks.

Russia



State-sponsored actors have enhanced their capabilities and targeted vulnerable U.S. infrastructure.

Iran



Threat actors are likely to target U.S. critical infrastructure in response to America's support of Israel.

North Korea



Threat actors continue targeting U.S. financial institutions, particularly cryptocurrency platforms.



Sector-Specific Risk Highlights

Healthcare & Public Health

Ransomware attacks are most prevalent in the Healthcare & Public Health sector, with high financial and patient care implications.

Information Technology

The Information Technology sector faces a constant barrage of ransomware and intrusion attempts, attempts, often exploiting vulnerabilities in educational systems.

Government Services & Facilities

Government facilities are vulnerable to ransomware and intrusion, particularly targeting local local governments and educational institutions.

Energy

The Energy sector faces threats from ransomware, data theft, and intrusions, with potential for potential for cascading effects across interconnected systems.

Risk Factor	Current State	Predictive Impact
Incident Response Planning	50% lack response/recovery plans	High likelihood of prolonged outages during cyber incidents. Expect increased severity of operational disruptions.
Multi-Factor Authentication (MFA)	50% do not use MFA	Increased risk of credential compromise. Predictable rise in successful phishing and ransomware attacks.
Third-Party Risk Management	Only 48% audit vendors, 39% engage in joint response planning	Third-party breaches will remain a top attack vector. Expect higher incidence of supply chain-based intrusions.
Cybersecurity Training	49% lack formal programs	Human error <u>likely</u> to remain a top cause of incidents. Anticipate preventable breaches due to phishing and misconfigurations.
Cyber Governance	44% lack a Chief Information Security Officer (CISO)	Strategic cybersecurity oversight is weak. Organizations without cyber leadership will lag in preparedness and incident coordination.
Tabletop Exercises	Only 48% conduct them biannually	Limited incident rehearsal will impair response time and effectiveness. Simulations

6 of the top 10 weaknesses in Risk Management areas

One year after state report released the Top-5 statewide NIST CSF weaknesses were unchanged with all trended slightly worse

Key Takeaways / Securing the Public Sector in 2025

- **Cyber threats are evolving faster than policies** – AI, quantum, and ransomware are raising the stakes.
- **People remain the most common entry point** – Social engineering, insider threats, and shadow AI must be addressed with training and tooling.
- **Legacy systems = future risk** – Aging infrastructure is a soft target for attackers. Modernization must include cybersecurity by design.
- **Zero Trust and Post-Quantum Readiness aren't optional** – They're foundational for long-term resilience and vendor compliance.
- **You can't secure what you can't see** – From Shadow IT to unmanaged devices, visibility is step one.
- **Cybersecurity is a shared responsibility** – Across agencies, vendors, and the community. Leadership matters.

The background of the slide is a dark, textured surface with a complex network of thin, glowing green and blue lines. These lines connect numerous small, white, circular nodes, creating a web-like pattern that resembles a digital or biological network. The lines and nodes are more densely packed in some areas, particularly towards the top and bottom edges, while the center is relatively clear, providing a space for the text.

Overview of the Florida Critical Infrastructure Protection Program @ USF

How to build your cyber and business resiliency?

1

Start the Florida
Cyber Risk
Assessment (FCRA)

2

Get Your Custom
Cyber Bulls-i
Resources and
Services

3

Manage Your Cyber
and Business
Journey with
Ongoing Support



1) Start the Florida Cyber Risk Assessment (FCRA)

A no-cost, Florida-specific assessment tool based on CSET®, designed to evaluate and enhance your cybersecurity posture.

Includes: 106 NIST Cybersecurity Framework (CSF 2.0) questions and 48 DHS Ransomware Readiness Questions

Delivers: Custom reports aligned with federal (NIST, DHS) and Florida Statute 282.3185
Integration with CIS Maturity Model Index & NICE workforce roles
Supports cybersecurity insurance readiness through risk identification and mitigation



2) Get Your Custom Cyber Bulls-i Resource Map



Automatically launched after completing the FCRA to give you targeted, actionable resources.



Simplifies complex NIST 800-series materials



Converts "No" answers into action steps and maturity



Maps no cost, state-provided tools to your unique risks



Reduces review time with tailored recommendations



3) Manage your Cyber and Business Journey with Ongoing Support

Use Cyber Florida's Journey Management
Pathway to guide long-term success.

Features:

Real-time progress
tracking &
dashboards

Personalized human
support

Resource
optimization &
situational awareness

No PHI or PII required



What You Get — All at No Cost:

7 customized reports to support strategic business planning

Access to templates, incident response guides, and maturity checklists

A 20-question entry-level assessment based on the top reported cybersecurity gaps across Florida

A 154-question full assessment aligned with NIST CSF 2.0 & DHS RRA

A Cybersecurity Incident Response Plan Template

Insight into Florida's top 5 cybersecurity workforce gaps (NICE TKS mapping)

Visualization tools to track progress and guide training priorities





CyberBulls-i

Florida's no-cost path to cyber resilience

Tailored Resources: Cyber Bulls-i (Infrastructure)

What is Cyber Bulls-i?

- Program to help stakeholders in all 16 critical infrastructure sectors in Florida
- Enhance Stakeholders cyber posture by offering them a portal to track their current state and access resources to close security gaps.
- Track their current state and access resources based on NIST SP800-53 to close security gaps
- Reduce time and allocate known and trusted resources - no cost to FL.
- Portal for respondents to complete their assessments, and access personalized resources offered by Cyber Florida and other providers to mitigate security weaknesses.

Score	Maturity Level <i>The recommended minimum maturity level is set at a score of 5 and higher</i>
7	Optimized: Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	Tested and Verified: Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	Implementation in Process: Your organization has formally documented policies, standards, and procedures and is in the process of implementation.
5	Risk Formally Accepted: Your organization has chosen not to implement based on a risk assessment.
4	Partially Documented Standards and/or Procedures: Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy.
3	Documented Policy: Your organization has a formal policy in place.
2	Informally Performed: Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.
1	Not Performed: Activities, processes and technologies are not in place to achieve the referenced objective.



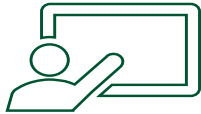
How did Cyber Bulls-i mapping tool come about?

- Results from the Florida Cyber Risk Assessment
- Respondents lacked time, funds and dedicated resources
- How are we measuring maturity and resiliency across all 16 sectors?
- Statewide feedback for support and resources
- Lack of due diligence after an assessment (follow up)
- Threat environment is more volatile and costly
- Small businesses cited costs and impact to business operations
- Supporting federal and State requirements and directives



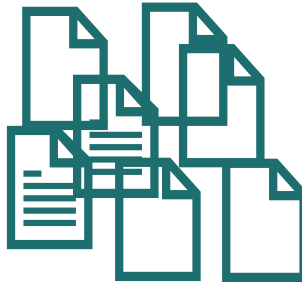
Summarize extracted information as CI resource for each item

FL Cyber Risk Assessment enhancements: Entry Assess (20-Q), Mid-level Assess (CPGs 38-Q), and CIS Maturity Index



FL Cyber Risk Assessment

Gaps



NIST 800-53 & other Cyber Standards mapped for 106 Questions

AI



Streamline

Targeted Resources

Maturity Scale

Re-assessments to track learning progress

CIS Maturity Scale implemented

✓ An Integrated new system

✓ Categorization of knowledge management resources

✓ Mapping resources to assessment results

✓ Sector wise learning models defined

✓ Sector specific reports and analysis

✓ Situational assessment data per CI sector





Emeka overview:



- Govern
- Identify
- Protect
- Detect
- Respond
- Recover

Module Question: RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared

Cybersecurity Plan Questions

Please answer the following questions. The resources below should help you understand how to answer the questions. Then, click *Next Module* or download all of your certification answers.

What is your organization's name?

Who will identify critical 3rd party suppliers and external partners (Name and contact)?

Download Plan Templates

Next Module

Resources to help you complete module RS.MA-01

Creating and executing an incident response plan with third-party coordination involves several key steps:

1. Establish the Plan

Develop a response plan that integrates your business continuity strategies and outlines roles, compliance requirements, and communication protocols. Update it regularly to reflect changes in the organization¹².

Module Question: RS.MA-02: Incident reports are triaged and validated

Cybersecurity Plan Questions

Please answer the following questions. The resources below should help you understand how to answer the questions. Then, click *Next Module* or download all of your certification answers.

Who is your incident command manager (Name and contact)?

[Download Plan Templates](#)[Next Module](#)

Module Question: RS.MA-03: Incidents are categorized and prioritized

Cybersecurity Plan Questions

Please answer the following questions. The resources below should help you understand how to answer the questions. Then, click *Next Module* or download all of your certification answers.

Who is your information technology/operational technology specialist (Name and contact)?

[Download Plan Templates](#)[Next Module](#)

Module Question: RS.MA-04: Incidents are escalated or elevated as needed

Cybersecurity Plan Questions

Please answer the following questions. The resources below should help you understand how to answer the questions. Then, click *Next Module* or download all of your certification answers.

Who will create your cybersecurity incident reporting procedure (Name and contact)?

[Download Plan Templates](#)[Next Module](#)

Governing laws, regulations and guidelines

Source	Regulation/Section
The Florida Senate	CS/HB 7055: Cybersecurity
NIST	NIST SP 800-61, rev 2

Policy statements

Incident handling capability

Cyber Florida Lake Show will develop and implement incident-handling capabilities to cover all information system components that fall within the scope of this policy. The incident handling capability will include a defined plan and procedure to handle all stages of cybersecurity incidents: preparation, detection, analysis, response, containment, and recovery.

Organizational roles and authorities

Cyber Florida Lake Show will define the organizational cybersecurity structure, roles, responsibilities, and levels of authority to handle cybersecurity incidents.

Incident reporting responsibility

Cyber Florida Lake Show will track, document, and report incidents to appropriate authorities as required by governing laws and regulations.

Prioritization and severity ratings of incidents

Cyber Florida Lake Show will define how it will assign a severity rating to cybersecurity incidents to critical cyber services and prioritize them for response and recovery.

Adopt and implement a cybersecurity risk management framework

Directly responsible individual (Name and contact): Anthony Davis

A Risk Management Framework (RMF) integrates security into the organization's business processes. The framework allows organizations to select the most effective security controls within the organization's budgetary and regulatory constraints. As a baseline, the NIST risk management framework (<https://csrc.nist.gov/projects/risk-management/about-rmf>) can be used as a starting point. Typically, the CISO or designee is responsible for selecting the risk management framework.

Identify critical suppliers and external partners

Directly responsible individual (Name and contact): LeBron James

Suppliers, their supply chains, and their products or services are a potential source of harm to critical cyber infrastructure. For example, a compromised device at an air-conditioning service company can insert malicious code into the organization when the compromised device connects to the organization's network to repair a defective AC unit. Important suppliers and external partners should be included in incident response planning. Typically, the purchasing organization is responsible for identifying critical suppliers and external partners.

Incident Response Plan (IRP)



CYBERSECURITY INCIDENT RESPONSE PLAN TEMPLATE

FOR SMALL AND MEDIUM PUBLIC + PRIVATE SECTOR ORGANIZATIONS



**CRITICAL
INFRASTRUCTURE
PROTECTION
PROGRAM**
UNIVERSITY OF SOUTH FLORIDA

Incident Response Plan (IRP) and Why You Need One:

- Cyberattacks are common — **every organization is a target.**
- A response plan helps:
 - Minimize downtime
 - Limit financial loss
 - Protect your reputation
- Many laws and regulations **require** a response plan (F.S. 282, HIPPA, etc)



Phased Approach

The 6 Phases of a Strong IRP



Form Your Response Team

- Identify key personnel (IT, legal, communications, leadership)
- Assign roles and responsibilities for each IR phase



Take Inventory of Assets

- Document critical systems, applications, and data
- Prioritize what needs to be protected and restored first



Define What Counts as an "Incident"

- Step-by-step instructions for each phase
- Use checklists or flowcharts – keep it simple



Establish Internal & External Communication Plans

- Who needs to be notified? When? How?
- Prepare template messages for employees, customers, regulators, etc.



Practice With a Tabletop Exercise

- Simulate a scenario to test the plan
- Involve all team members and take notes on gaps or confusion



Document and Store the Plan Accessibly

- Keep it in multiple locations (digital and physical)
- Make sure team members know where to find it



Incident Response Planning Guide

This document is intended to help small organizations be better prepared to respond to and recover from cybersecurity incidents. Aligned to the standards of the National Institute of Standards and Technology (NIST), this guide can be used to help your organization establish an incident response policy.

Download the fillable MS Word form and complete it with your senior leadership team to help your organization be more prepared to mitigate and recover from a cyber incident.

DOWNLOAD THE INCIDENT
RESPONSE PLANNING GUIDE >>

Cyber Decision-Making Matrix

This document (an MS Excel sheet) developed in partnership with the Florida Department of Emergency Management can help local government and other critical infrastructure organizations determine who is responsible for various areas of response *before* a cyber incident occurs. Review the list of likely actions needed in the wake of a cyber incident and assign roles in advance for a more coordinated response when the need arises.

DOWNLOAD THE CYBER
DECISION-MAKING MATRIX >>

Situation Manual Development Tabletop Exercise

Developed in partnership with the Florida Department of Emergency Management, use this guide (an MS Word doc) to host your own tabletop exercise with organizational leaders, helping them learn to plan and design an organizational situation manual for responding to a cyber incident. Assign roles and play through the exercise to explore some of the considerations and decisions an organization faces in the wake of cyber incident. Use the experience to help develop a situation manual for your organization.

DOWNLOAD THE SITUATION
MANUAL TTX >>

Cybersecurity Emergency Support Function (ESF) Directory

Developed in partnership with the Florida Department of Emergency Management, the Cybersecurity Emergency Support Function Directory (an MS Word doc) is a repository for the state-provided support services available to you before, during, and after a cyber incident. Use this guide to help identify critical emergency actions and how to coordinate with appropriate state agencies during a cyber emergency.

DOWNLOAD THE ESF
DIRECTORY >>



On Behalf of Cyber Florida...





END