



# AN INITIATIVE TO STRENGTHEN FLORIDA'S CRITICAL INFRASTRUCTURE

CRITICAL INFRASTRUCTURE RISK ASSESSMENT (CIRA)

2022-2023

# CYBER FLORIDA AND PARTNERS

- The Florida Center for Cybersecurity (aka Cyber Florida) was created by the State in 2014 and hosted by the University of South Florida
- Help Florida become a national leader in cybersecurity education, academic and practical research, and community outreach and engagement
- Build a robust pipeline of future professionals by introducing cyber safety and career awareness programs to K–12 schools



# CYBER FLORIDA PROGRAMS

Degree and Certificate Program – work with all 12 SUS in Florida to provide education and certification in cybersecurity

CyberWorks Carrier Training – workforce development initiative offering a 19-week certificate course. Receive free vouchers to take CompTIA Networking + and CompTIA Cybersecurity Analyst (CySA+) certification tests.

Go to [Cyberflorida.org](https://Cyberflorida.org) for more information on these programs!







# WHY ARE WE DOING THIS?

State of Florida Appropriation 2944B FY 2023 states that Cyber Florida shall conduct a risk assessment of the state's critical infrastructure (CI) and submit a draft report by 9 Jan 2023 and a final report with actionable solutions to improve the state's preparedness and resilience to significant cybersecurity incidents by 30 Jun 2023.

# WHAT ARE WE EVALUATING?

- 16 Critical Infrastructure + Subsectors
- The threat landscape for cyberattacks
- Establish a baseline of current CI cybersecurity protections and provide actionable solutions to State leaders

# TIMELINE AND DELIVERABLES

					
<b>October 2022</b> Survey opens for Phase 1	<b>December 15, 2023</b> Phase 1 survey deadline	<b>January 1, 2023</b> Survey opens for Phase 2	<b>January 9, 2023</b> Preliminary report submitted	<b>May 31, 2023</b> Phase 2 survey deadline	<b>June 30, 2023</b> Final report submitted

- Florida Cybersecurity Risk Assessment Tool:
  - A state-wide confidential/anonymous survey to measure the state’s critical infrastructure using Idaho National Laboratory (INL)-developed Cybersecurity Evaluation Tool (CSET®)
  - Cyber Florida CSET® Instance is now live for Phase 2!
- Outreach:
  - Communications
  - Engagements
  - Educational platforms
- Reporting:
  - A preliminary report by 9 January 2023
  - A final report with actionable solutions shared with Legislative Leaders, the Governor, and FL Cybersecurity Advisory Council by 30 June 2023

# EARLY TRENDS AND RECOMMENDATIONS

**FBI - In 2022 Cyber Crimes impacted nearly 43K Floridians, stealing nearly \$845M, 2<sup>nd</sup> to California**



**49%** have a formal cybersecurity training program



**45%** or less leverage Two-factor authentication implemented for all users



Less than **50%** test response and recovery plans with third party providers



Implement recurring micro-grant program to support technology purchases and upgrades and personnel training and upskilling



Invest in workforce development and critical infrastructure



Develop sustained CI cyber security support, funding and training to Florida public and private sectors

# USF CYBERSECURITY

- The University of South Florida (USF) uses the NIST Cybersecurity framework to manage its technical and administrative controls used at the university.
- The USF has a complete set of Security Policies, procedures, and standards based on the NIST 800-171 security guidelines.
- Technical controls: Several Physical and Cloud based Palo Alto Firewalls, the complete Microsoft Defender Stack of products including EDR, Beyond Trust Privileged access management, Microsoft MFA, Splunk for Enterprise Security SIEM, and regular penetration tests and risk assessment performed by both internal staff, state auditors, and 3rd party companies.
- The USF is a Carnegie Research-1 University with numerous federal grants dealing with Medical, Personal, and DoD restricted non classified data that is secured and monitored 24/7 by USF staff as well as 2 external SOCs.

# CYBER SECURITY EVALUATION TOOL (CSET®)



- Developed by INL for DHS Cybersecurity & Infrastructure Security Agency (CISA)
- Stand-alone desktop application that guides asset owners and operators through a systematic and repeatable approach for assessing an organization's cybersecurity posture
  - Information Technology (IT)
  - Operational Technology (OT) cyber security
- Identifies cyber security strengths and deficiencies based on industry standards
- Derives security enhancement recommendations from database of cybersecurity standards, guidelines, practices and associated actions

18 years of DHS development and refinement  
Almost 100,000 overall downloads



**CSET®**  
CYBER SECURITY EVALUATION TOOL




# CYBER SECURITY EVALUATION TOOL (CSET®)




- Provides a method to systematically compare and monitor security improvements in cyber systems
- June 2021: CSET® was updated (Version 12) to include a new module: Ransomware Readiness Assessment (RRA)
  - Self-assessment based on a tiered set of practices
  - Helps organizations better assess how well they are equipped to defend against and recover from a ransomware incident
- Questions are weighted by cybersecurity experts from INL

# CYBER FLORIDA CSET® INSTANCE



Enter your email address and password to login.



Enter your email address and password to login.

Email

Password

[Login](#) [Reset Password](#) [Register New User Account](#)

Thank you for participating in the CyberSecureFlorida initiative, a first-of-its-kind effort to assess the cybersecurity strengths and weaknesses of Florida's collective critical infrastructure. The information gathered through this effort will be essential to helping Florida's elected leaders determine how best to allocate resources and enact appropriate legislation to create a more secure Sunshine State! CyberSecureFlorida is open to all public- and private-sector critical infrastructure entities, and we encourage any and all critical infrastructure entities to lend their voice to this important undertaking.



Assessment Name	Assessment Type	Last Modified	Primary Assessor	Status	
<a href="#">New Assessment</a>	RRA, Cybersecurity Framework	07 Nov 2022		48/156 Question(s) Completed	<a href="#">Remove</a> <a href="#">Export</a> <a href="#">Analytics</a>
<a href="#">New Assessment</a>	RRA, Cybersecurity Framework	07 Nov 2022		0/156 Question(s) Completed	<a href="#">Remove</a> <a href="#">Export</a> <a href="#">Analytics</a>
<a href="#">New Assessment</a>	RRA, Cybersecurity Framework	07 Nov 2022		0/156 Question(s) Completed	<a href="#">Remove</a> <a href="#">Export</a> <a href="#">Analytics</a>

Agency cybersecurity information, exempt pursuant to Florida Statute Chapter 119 Section 119.0725 | Cyber Florida | Contact Cyber Florida at: [secureflorida@cyberflorida.org](mailto:secureflorida@cyberflorida.org)

Hosted on University of South Florida (USF) system

# CYBER FLORIDA CSET® INSTANCE

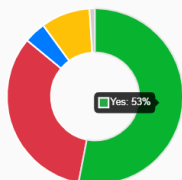
Tailored CSET® instance comprised of:

- Assessment Information (9 questions)
  - Infrastructure Taxonomy
  - Geographic Operations
  - Consequence
- Cybersecurity Framework Standard Questions (108 Questions)
  - Protect
  - Detect
  - Identify
  - Respond
  - Recover
- Ransomware Readiness Assessment (48 Questions)
  - 10 performance goals

7 different submitter reports available immediately

# CYBERSECURITY FRAMEWORK STANDARD QUESTIONS RESULTS

## Analysis Dashboard



### Score

Overall Score	Standard-based
64%	64%

## Control Priorities

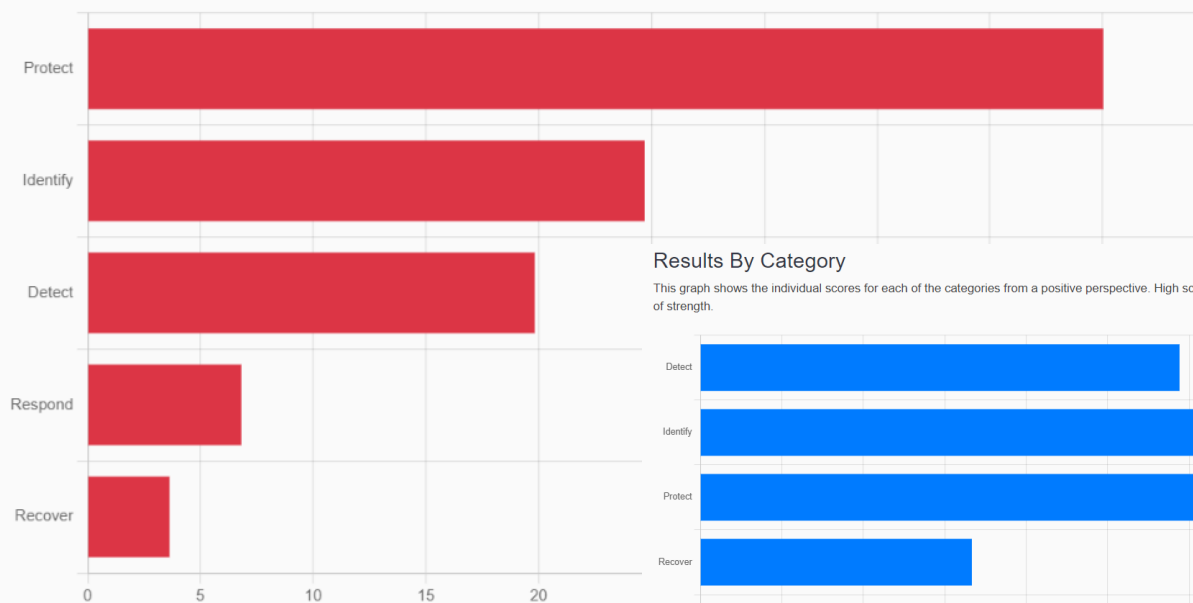
Information on ranking can be found in the [User Guide](#).

<b>Standard:</b> Cybersecurity Framework	<b>Rank</b>
<b>Category:</b> Protect	<b>1</b>
<b>Answer:</b> No	
<b>Question</b>	<b>Reference #</b> PR.MA-2
Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	

<b>Standard:</b> Cybersecurity Framework	<b>Rank</b>
<b>Category:</b> Protect	<b>2</b>
<b>Answer:</b> No	
<b>Question</b>	<b>Reference #</b> PR.AC-5
Network integrity is protected, incorporating network segregation where appropriate	

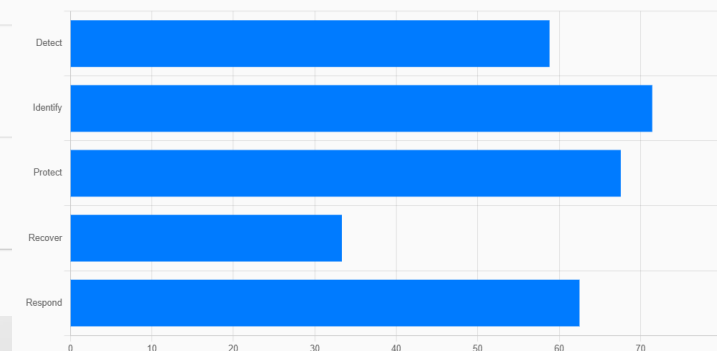
## Top Ranked Categories

This graph shows the top areas of concern ranked. These are calculated from a weighted risk score based on the difficulty of attack. The attack weights are most heavily weighted for easy attacks to less for more difficult to attack.



## Results By Category

This graph shows the individual scores for each of the categories from a positive perspective. High scores on this graph show areas of strength.

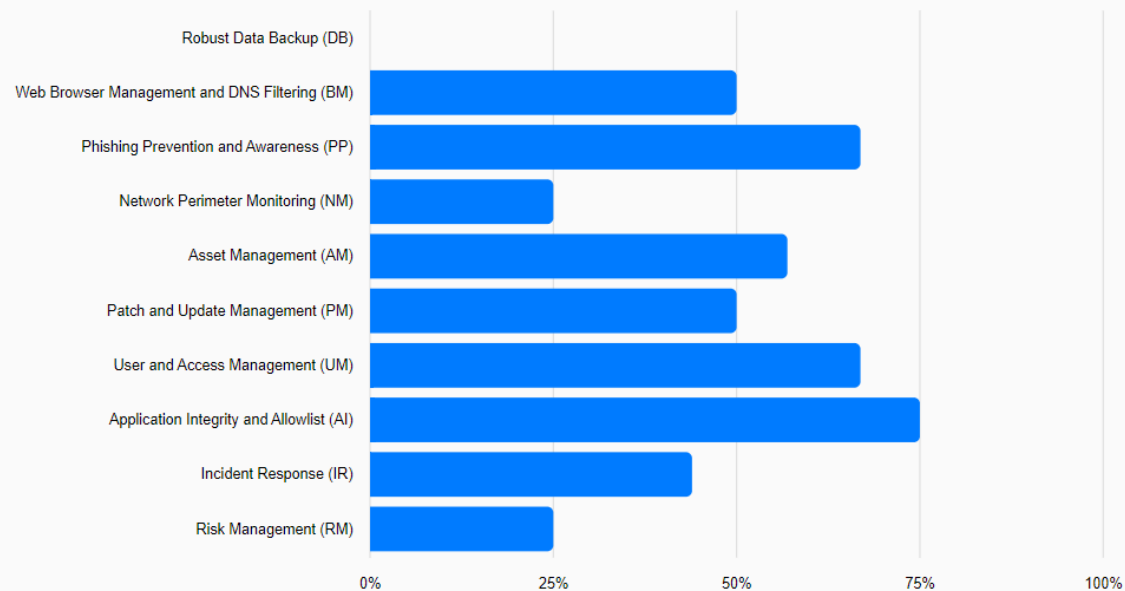


# RANSOMWARE READINESS ASSESSMENT RESULTS

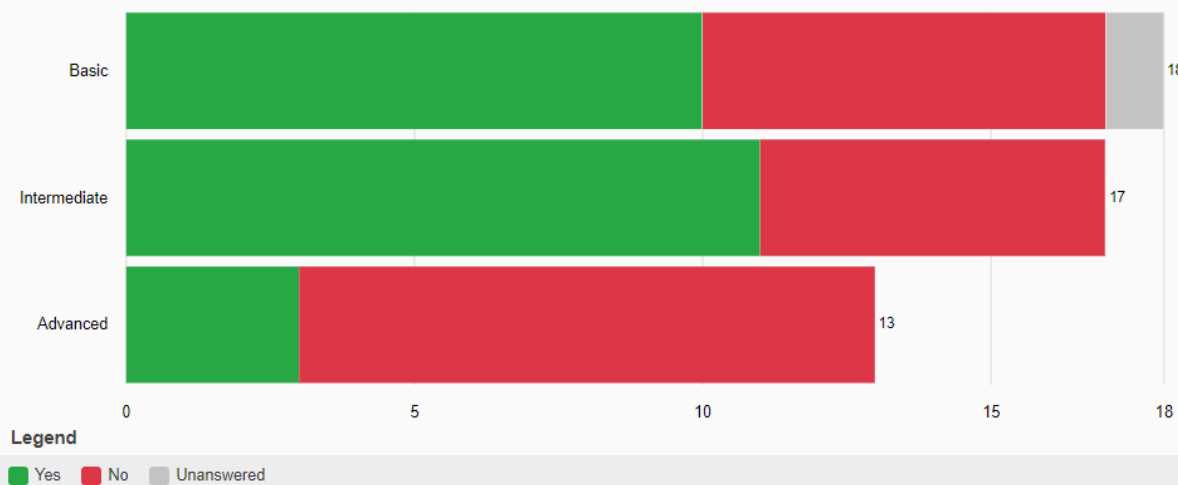
## Goal Performance

### RRA Performance by Goal

This chart shows your positive assessment results. High scores on this chart are desirable.



### Practices Answered Per Tier



# BENEFITS OF PARTICIPATION

- Evaluate
  - Systematic, disciplined, and repeatable approach for evaluating cybersecurity posture
  - Focused on IT and OT cybersecurity
  - Ransomware-specific assessment
- Tailored reporting
  - Compare cyber risks across infrastructure sectors with interactive visualization capability
  - Anonymized state-wide summary report
- Reasonable level of effort
  - No cost
  - Low time commitment
  - Free analysis related to education and training resources
  - Points given to your FL Cybersecurity grant application

# WHERE DO WE GO FROM HERE?

## *DEVELOP THE CYBERSECURITY WORKFORCE*

- Do you have staff with the knowledge and skills to address the gaps revealed in your organization's CSET assessment? How do you know?
- Known risks in cybersecurity workforce development include:
  - Poaching/retention
  - Compliance needs
  - Understanding organizational hiring needs
  - Recruiting qualified staff

# WHAT IS CYBERKNIGHTS?

CyberKnights is a cybersecurity career center aligned to the NIST-NICE Framework that is at the crossroads of educators, employers, and individuals.

## Educators



Understand employer needs



Forecast educational needs



Connect with students

## Employers



Identify Skills Gaps



Recruit New Talent



Retain Employees

## Individuals



Assess and Showcase Skills



Chart Unique Path



Keep Developing Talent



# HOW DOES CYBERKNIGHTS SUPPORT FLORIDA'S CRITICAL INFRASTRUCTURE RISK ASSESSMENT?

Step 1:

Import CSET file →

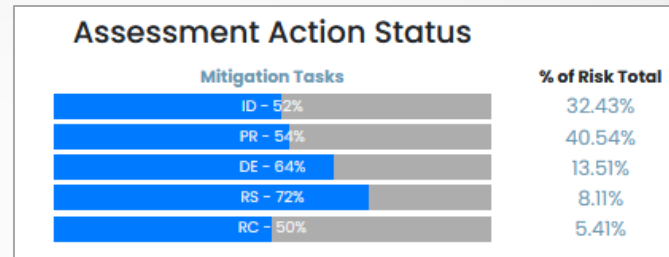
**Upload CSET File**

**File**  No file selected.

**Accepted File type:** .csv  
**Max File Size:** 5MB

Step 2:

CSET Risk Assessment Action Status →



Step 3:

Skills to mitigate risks identified for talent search →

Candidate	Current Institution	Highest Education	Major Study	Minor Study	Career Level	Military Status	Willing To Relocate	K&Ss Matched
Jimmy Winter		Bachelor's			Experienced/Manager	Disabled		95%
Lee Ma		Bachelor's					Yes	83%
Ford Steele		High School/GED			Entry Level	Undisclosed	Yes	82%
Landen Willions		Bachelor's	Computer Science	robotics	Entry Level	No		82%

Step 4:

Understand aggregate employer needs and forecast future educational needs across the state of Florida to mitigate critical infrastructure risk

# GOING DEEPER: OPPORTUNITY FOR CRITICAL INFRASTRUCTURE OWNERS/OPERATORS

Select number of participants offered CyberKnights service for free

- Cybersecurity improvement areas identified from the risk assessment submitted
- Identifies knowledge and skills necessary to mitigate cyber risks within the submitter's agency, organization, or company
- Access to full suite of cyber workforce development toolsets that will identify skills gaps, training pathways, and finding the most qualified new cyber talent
- Provides information related to education and training courses

To be considered for the no-cost analysis, interested participants must fully complete their Cyber Florida CSET risk assessment and indicate interest within the CSET.

#### Additional Cybersecurity Risk Service

In addition to the CSET reports available, Cyber Florida will provide a select number of participants with information directly related to education and training courses that target the cybersecurity improvement areas identified from the risk assessment information submitted. The free service will also identify the knowledge and skills necessary to mitigate cyber risks within the submitter's agency, organization, or company. Additionally, the selected participants will have free access to a full suite of cyber workforce development toolsets that will identify skills gaps, display various training pathways for upskilling employees, and assist with finding the most qualified new cyber talent, if needed. To be considered for the no-cost analysis, interested participants must fully complete their CSET risk assessment.

Are you interested in being considered for this free assessment follow-on service?

- Yes
- No
- Maybe Later

# Why is MITRE involved in CIRA?

## MITRE Operates Six Federally Funded Research & Development Centers (FFRDCs)

Mission-driven in the public interest

Objective & conflict free insight (not-for-profit)

Unique Vantage Point

Technical Know-How

Pioneering Together

Our Mission is to **solve problems for a safer world**. At MITRE, we work across the whole of government on big problems that challenge our nation's stability. We strive to earn the trust of our sponsors and partners so that we may have **greater impact for public good**.

MITRE



# NEXT STEPS

- Complete and submit the CSET® assessment
- Print or download your individual risk assessment reports
- Leverage existing and near future resources from Cyber Florida and INL
- **Multiple surveys for each entity i.e.,** water, wastewater, transportation, tax collector, courts, elections, etc.
- **Comparison data** within your sector
  
- **Share with your vendors, contractors, suppliers, etc.**
- **Help inform the legislature of the most urgent need of funding and resources**
- **More information - [Cybersecureflorida.org](https://cybersecureflorida.org) and “Assistance Calls with Experts to Complete the CSET” Thursday at 1:00 pm**

# QUESTIONS/COMMENTS?

**CYBERSECUREFLORIDA.ORG**

Bryan Langley  
bjlangley@cyberflorida.org

Emilio F Salabarria  
esalabarria@cyberflorida.org