Cyberattacks:
Cyber Defenses from the MS-ISAC and Current Regulatory Requirements

Dan O'Hagan
Deputy General Counsel & Manager of Regulatory Compliance
Florida Municipal Power Agency

Megan Incerto
Regional Engagement Manager
Center for Internet Security

Cyberattacks: Cyber Defense from the MS-ISAC and Current Regulatory Requirements

FMEA Annual Conference

August 1, 2024


CIP
MS-ISAC
NERC
CIRCIA

Presentation Overview

- Part I – Overview of Recent Federal & State Cybersecurity Laws/Regulations
  - CIRCIA
  - NERC CIP Standards
  - Florida HB 7055 (2022)
  - Florida HB 7057 (2022)
- Part II – Cyber Defenses from the MS-ISAC
  - MS-ISAC Overview
  - Cyber Threat Trends
  - CIS Controls, Tools & Best Practices

FMPA MUNICIPAL POWER

Recent Federal Cybersecurity Laws/Regulations

Federal Cybersecurity Laws

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

- CIRCIA Signed by President Biden March 2022
  - Covered entities must report to Cybersecurity & Infrastructure Security Agency ("CISA") any cyber incidents within 72 hours and ransomware payments within 24 hours
- Requires CISA to begin rulemaking process to develop and implement rules
  - NOPR issued April 4, 2024
  - Comment period closed July 3, 2024
  - APPA (with FMPA, FMEA member input) filed comments
  - Final rule expected around August 2025 (= 18 months after NOPR)

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Cyber Incident Reporting for Critical Infrastructure Act of 2022 Publication

PUBLICATION

Download File (PDF, 149.47 KB)

Cyber Incident Reporting for Critical Infrastructure Act of 2022 - Notice of Proposed Rulemaking Informational Overview

PUBLICATION

This is an unofficial, informational resource summarizing aspects of the CIRCIA Notice of Proposed Rulemaking (NPRM) created to assist stakeholders in reviewing the NRPM.

Download File (PDF, 631.32 KB)

https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

FMPA MUNICIPAL POWER

CIRCIA Continued

Proposed Rule – Key Definitions

- "Covered entities" broadly defined to include:
  1. Any entity that exceeds the Small Business Administration's "Small Business" regs
     - = Around 1,000 employees for electric utilities
  2. Any entity required to report under NERC CIP Reliability Standards
     - Includes BAs, GOs, GOPs, RCs, TOs, TOPs, and some DPs
  3. Catch-all – Any entity required to file DOE Form 417 "Electric Emergency Incident and Disturbance Report"
     - Broadly defined to include all public power utilities.
       - "A corporation, person, agency, authority, or other legal entity or instrumentality aligned with distribution facilities for delivery of electric energy for use primarily by the public. Included are investor-owned electric utilities, municipal and State utilities, federal electric utilities, and rural electric cooperatives."

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

FMPA MUNICIPAL POWER

CIRCIA Continued

Proposed Rule – Key Definitions

- "Cyber incident" means "an occurrence that actually jeopardizes…the integrity, confidentiality, or availability of information on an [IT or OT] system; or actually jeopardizes, without lawful authority, an [IT or OT] system."
- "Substantial cyber incident" broadly defined to include "cyber incidents" that results in:
  - Loss of confidentiality, integrity, or availably of information systems or network
  - Serious impact on the safety or resiliency of operational systems and processes
  - Disruption in ability to engage in business or industrial operations,
  - Unauthorized access that is facilitated through or caused by compromised cloud service or other third-party provider or supply chain components.

  Note that this definition if broader than current CIP and DOE-417 reporting requirements.
- "Ransomware attack" / "ransom payment" essentially defined as a use or threat of a cyber incident to extort a demand for a ransom payment

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Cyber Incident Reporting for Critical Infrastructure Act of 2022 Fact Sheet

PUBLICATION

Download File (PDF, 302.05 KB)

Covered Cyber Incident Fact Sheet

FACT SHEET

Under the CIRCIA NPRM, a covered entity that experiences a covered cyber incident is required to report. Find out what covered cyber incident are.

Download File (PDF, 349.69 KB)

https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

FMPA MUNICIPAL POWER

CIRCIA Continued

APPA Comments & Next Steps

- APPA Comments:
  - "Covered entities" definition too broad. Captures very small public power utilities with little/no impact on reliability
  - Reduce duplicative reporting requirements
  - Utility size should be factored into "substantial cyber incident"
  - Other clarifying changes
- Final rule expected 18 months after NOPR publication (= August 2025)

FMPA MUNICIPAL POWER

Federal Cybersecurity Laws
NERC Reliability Standards

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- NERC "CIP" Standards
  - "Suite of standards" addressing Cybersecurity
  - CIP-003-8 – "Cyber Security – Security Management Controls"
  - CIP-008-6 – "Cyber Security – Incident Reporting and Response Planning"
    - BA, GO, GOP, RC, TO, TP, & some DPs
    - High & Medium Impact Facilitates
    - Generally requires entities to have Incident Response Plan and to report certain cyber incidences or attempts to E-ISAC utilizing Form DOE-417
- NERC EOP-004-4 – "Event Reporting"
  - Related to physical events, but may implicate cybersecurity.
  - Utilizes Form DOE-417

FMPA MUNICIPAL POWER

Federal Cybersecurity Laws

DOE-417 - Electric Emergency Incident and Disturbance Report

U.S. Department of Energy Form DOE-417	*ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT*	OMB No. 1901-0288 Approval Expires: 05/31/2024 Burden Per Response: 1.8 hours

NOTICE: This report is **mandatory** under Public Law 93-275. Failure to comply may result in criminal fines, civil penalties and other sanctions as provided by law. For the sanctions and the provisions concerning the confidentiality of information submitted on this form, see General Information portion of the instructions. **Title 18 USC 1001 makes it a criminal offense for any person knowingly and willingly to make to any Agency or Department of the United States any false, fictitious, or fraudulent statements as to any matter within its jurisdiction**.

RESPONSE DUE:

Within 1 hour of the incident, submit Schedule 1 and lines N - S in Schedule 2 as an Emergency Alert report if criteria 1-9 are met. If criterion 2 is met, also submit the Cyber Attributes on line T in Schedule 2.
Within 6 hours of the incident, submit Schedule 1 and lines N - S in Schedule 2 as a Normal Report if only criteria 10-13 are met.
By the end of the next calendar day after a determination, submit Schedule 1 and lines N – S and the Cyber Attributes on line T in Schedule 2 as an Attempted Cyber Compromise if criterion 14 is met.
By the later of 24 hours after the recognition of the incident OR by the end of the next business day submit Schedule 1 and lines N - S in Schedule 2 as a System Report if criteria 15-26 are met. *Note: 4:00pm local time will be considered the end of the business day*

Submit updates as needed and/or a final report (all of Schedules 1 and 2) within 72 hours of the incident.

For NERC reporting entities registered in the United States; NERC has approved that the form DOE-417 meets the submittal requirements for NERC. There may be other applicable regional, state and local reporting requirements.

METHODS OF FILING RESPONSE
(Retain a completed copy of this form for your files.)

Online: Submit form via online submission at: https://www.oe.netl.doe.gov/OE417/
FAX: FAX Form DOE-417 to the following facsimile number: (202) 586-8485.
Alternate: If you are unable to submit online or by fax, forms may be e-mailed to doehqeoc@hq.doe.gov, or call and report the information to the following telephone number: (202) 586-8100.

FMPA MUNICIPAL POWER

SCHEDULE 1 -- ALERT CRITERIA

(Page 1 of 4)

Criteria for Filing (Check all that apply) – See Instructions For More Information

EMERGENCY ALERT **File within 1-Hour** If any box 1-9 on the right is checked, this form must be filed within 1 hour of the incident; check Emergency Alert (for the Alert Status) on **Line A** below.	1. [ ] Physical attack that causes major interruptions or impacts to critical infrastructure facilities or to operations 2. [ ] Reportable Cyber Security Incident 3. [ ] Cyber event that is not a Reportable Cyber Security Incident that causes interruptions of electrical system operations. 4. [ ] Complete operational failure or shut-down of the transmission and/or distribution electrical system 5. [ ] Electrical System Separation (Islanding) where part or parts of a power grid remain(s) operational in an otherwise blacked out area or within the partial failure of an integrated electrical system 6. [ ] Uncontrolled loss of 300 Megawatts or more of firm system loads for 15 minutes or more from a single incident 7. [ ] Firm load shedding of 100 Megawatts or more implemented under emergency operational policy 8. [ ] System-wide voltage reductions of 3 percent or more 9. [ ] Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System
NORMAL REPORT **File within 6-Hours** If any box 10-13 on the right is checked AND none of the boxes 1-9 are checked, this form must be filed within 6 hours of the incident; check Normal Report (for the Alert Status) on **Line A** below.	10. [ ] Physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which targets components of any security systems 11. [ ] Cyber event that could potentially impact electric power system adequacy or reliability 12. [ ] Loss of electric service to more than 50,000 customers for 1 hour or more 13. [ ] Fuel supply emergencies that could impact electric power system adequacy or reliability
ATTEMPTED CYBER COMPROMISE **File within 1-Day** If box 14 on the right is checked AND none of the boxes 1-13 are checked, this form must be filed by the end of the next calendar day after the determination of the attempted cyber compromise; check Attempted Cyber Compromise (for the Alert Status) on **Line A** below.	14. [ ] Cyber Security Incident that was an attempt to compromise a High or Medium Impact Bulk Electric System Cyber System or their associated Electronic Access Control or Monitoring Systems

FMPA MUNICIPAL POWER

Recent Florida Cybersecurity Laws/Regulations

Florida Cybersecurity Laws

House Bill 7055 ("Cybersecurity Reporting Bill")

- Creates new "Local Government Cybersecurity Act," codified in section 282.3185, Florida Statutes.
- Four key components:
  1. Cybersecurity reporting requirement
  2. No paying cyber ransom
  3. Cybersecurity training requirements
  4. Develop/Adopt cybersecurity standards

FMPA MUNICIPAL POWER

Florida Cybersecurity Laws

Local Government Cybersecurity Act (s. 282.3185, Fla. Stat.)

1. Cybersecurity Reporting Requirement

- Municipalities must report cybersecurity incidents (48 hours) and ransomware incidents (12 hours) to (1) the Cybersecurity Operations Center, (2) Cybercrime Office of the Department of Law Enforcement, and (3) the sheriff who has jurisdiction over that municipality.
- Statues defines key terms such as “incident,” “ransomware incident,” and prescribes the information that must be reported.
  - **Note: Definitions do not match or reference CIRCIA, NERC Standards, or DOE-417**

2. No Paying Cyber Ransom

- “a municipality experiencing a ransomware incident may not pay or otherwise comply with a ransom demand.” Fla. CS for HB 7055, § 4 (2022) (proposed § 282.3186, Fla. Stat.) (emphasis added).

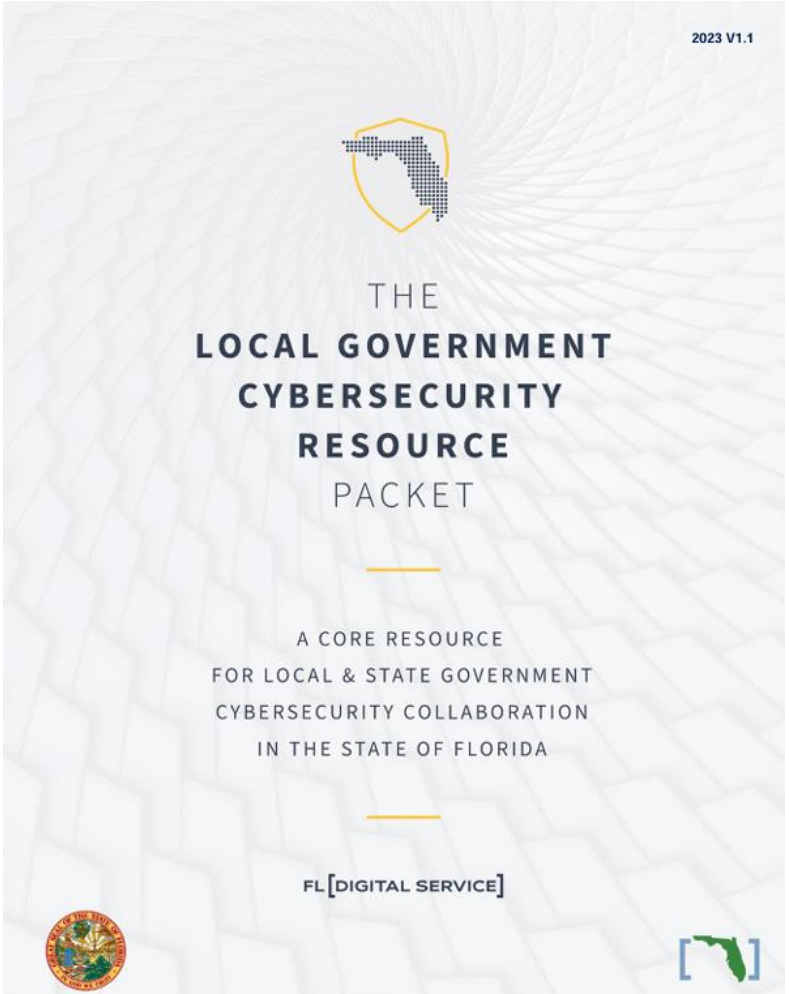
FMPA MUNICIPAL POWER

Florida Cybersecurity Laws

Local Government Cybersecurity Act (s. 282.3185, Fla. Stat.)

3. Cybersecurity Training Requirements

- Basic training for all employees, and advanced cybersecurity training for those with access to “highly sensitive information” is required
  - Training curriculum to be developed by Florida Digital Service
  - Cities and counties must train all employees 30 days of beginning employment and annually thereafter.



https://digital.fl.gov/cybersecurity/

FMPA MUNICIPAL POWER

Florida Cybersecurity Laws

Local Government Cybersecurity Act (s. 282.3185, Fla. Stat.)

4. Develop/Adopt Cybersecurity Standards

- Cities must develop and adopt cybersecurity standards designed to "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 National Institute of Standards and Technology Cybersecurity Framework."
  - Population of 25,000 or more deadline = January 1, 2024
  - Population of 25,000 or less deadline = January 1, 2025

FMPA MUNICIPAL POWER

New Florida Critical Infrastructure Protections

FL House Bill 275 (2024); New s. 812.141, Florida Statutes

- Criminalizes unauthorized electronic access to and tampering with computers, systems, networks, or electronic devices of "critical infrastructure entities"
  - "Critical infrastructure entities" broadly defined to include municipal electric utilities and their distribution/transmission facilities and computer systems/networks/devices.
  - Unauthorized access = Third degree felony
  - Tampering = Second degree felony

FMPA MUNICIPAL POWER

Florida Cybersecurity Laws

House Bill 7057 ("Open Government Bill)

- Creates **new public records exemption** (sec. 119.0725, Fla. Stat.) for:
  - Cybersecurity insurance coverage, limits and deductibles, and risk mitigation measures:
    - "coverages acquired for the protection of information technology systems, operational technology systems, or data . . . ."
    - Information relating to critical infrastructure.
      - Here, "critical infrastructure" is defined to mean existing information technology (IT) or operational technology (OT) systems and assets, whether physical or virtual, where their incapacity or destruction would have a negative impact on security, economic security, public health, or public safety."
    - Cybersecurity incident information reported to the State and other reporting agencies.
    - Network information (including schematics, hardware and software configurations, and encryption information) that would facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of data or information; or IT resources, including existing and proposed IT systems.

Florida Cybersecurity Laws

House Bill 7057 ("Open Government Bill (cont'd)

- Creates **new open/public meeting exemption** (sec. 282.318(6), Fla. Stat.) for:
  - All of the information subject to public records exemption above.
- Any "shade" meeting to discuss exempt information must be recorded and transcribed.
- Exempt information remains available to law enforcement & other gov't agencies.

Questions on State/Federal Cybersecurity Laws/Regs?

Dan O'Hagan
FMPA Deputy General Counsel & Manager of Regulatory Compliance
FMEA Legal Counsel
Dan.ohagan@fmpa.com
850-297-2011

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Cyber Defenses From the MS-ISAC

Megan Incerto

Regional Engagement Manager, MS-ISAC

Megan.Incerto@cisecurity.org | 518-640-3655

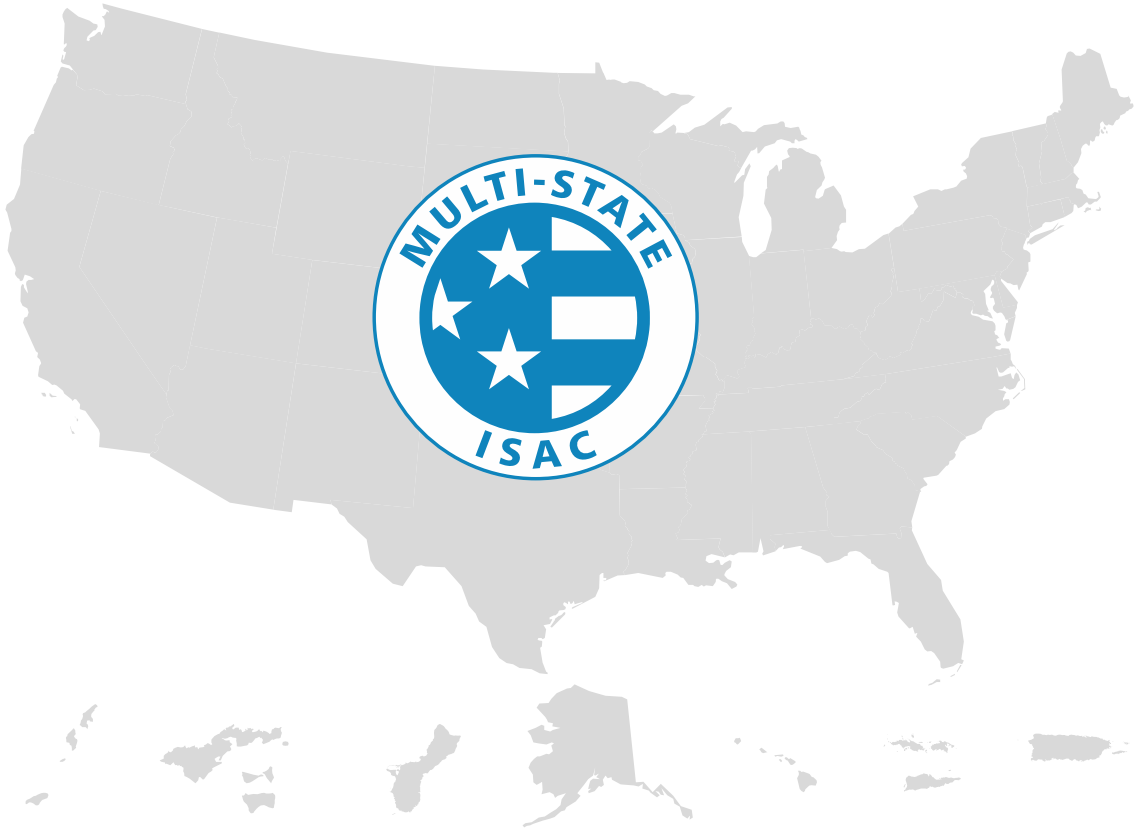
MS-ISAC®

Multi-State Information Sharing & Analysis Center®

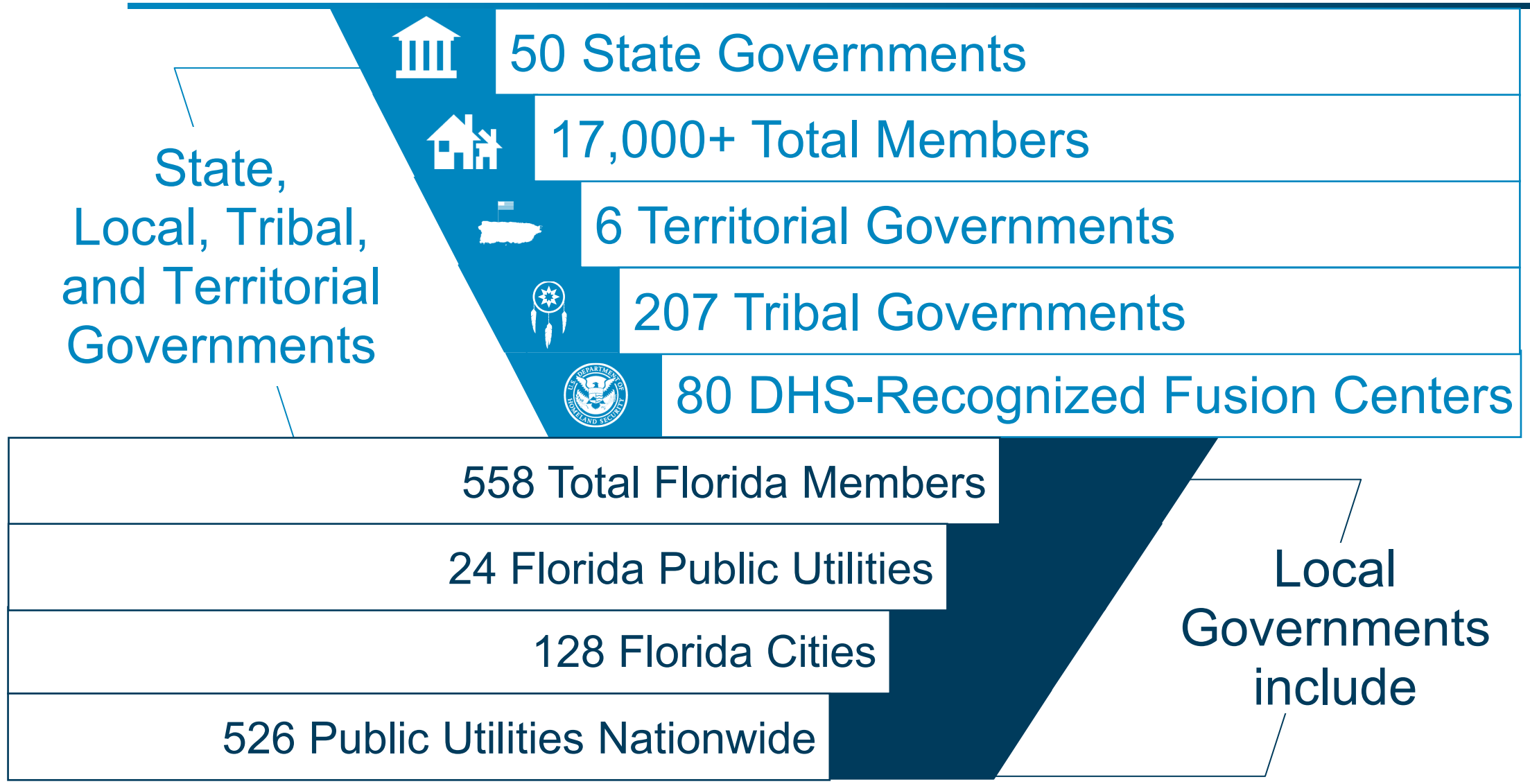
The MS-ISAC®

- Designated by the Cybersecurity & Infrastructure Security Agency (CISA) as a key resource for cyber threat prevention, protection, response and recovery for all U.S. State, Local, Tribal and Territorial (SLTT) governments.
- A division of the Center for Internet Security® (CIS®), a 501(c)(3) nonprofit.

https://learn.cisecurity.org/ms-isac-registration



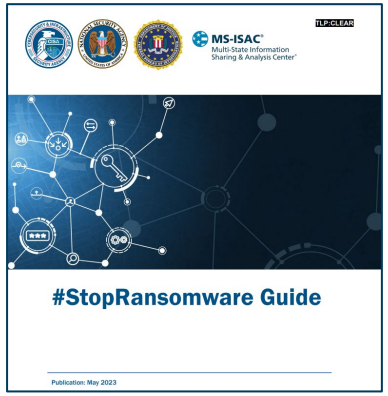
Who We Serve


State, Local, Tribal, and Territorial Governments
50 State Governments
17,000+ Total Members
6 Territorial Governments
207 Tribal Governments
80 DHS-Recognized Fusion Centers
558 Total Florida Members
24 Florida Public Utilities
128 Florida Cities
526 Public Utilities Nationwide
Local Governments include

Recommendations for SLTTs

Preparation is Key

- **#StopRansomware Guide**
  - Best practices and incident response guidance
  - Joint guide (CISA, FBI, NSA, and MS-ISAC)



- **CIS Critical Security Controls**
  - Provide a prioritized set of actions to protect your organization and data from known cyber-attack vectors

CIS Controls

- **CIS Community Defense Model 2.0**
  - How effective are the CIS Controls against the most prevalent types of attacks?

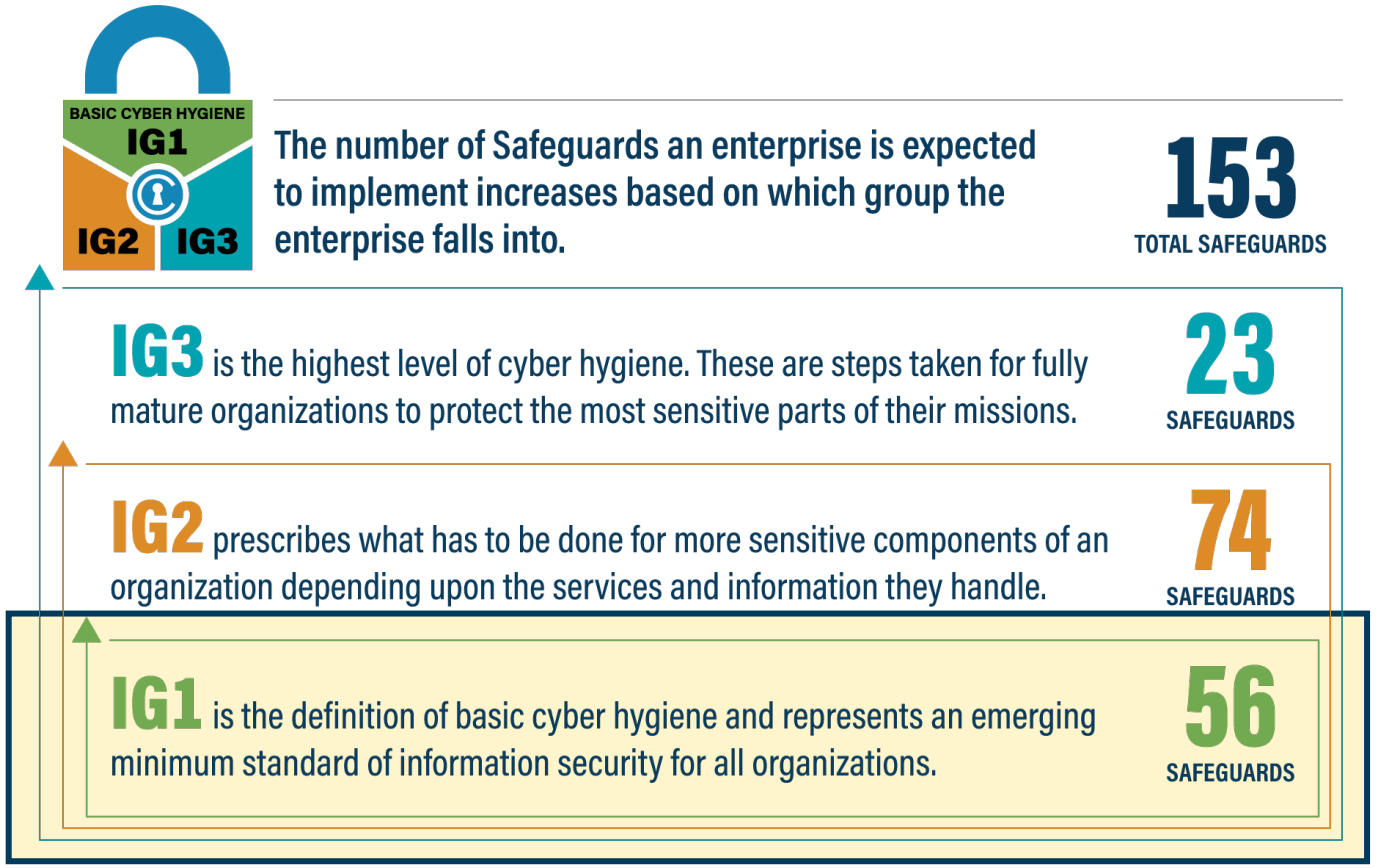
Top 5 Attacks	IG1 CIS Safeguards IG1 can defend against XX% of ATT&CK (Sub-)Techniques	All CIS Safeguards CIS Safeguards can defend against XX% of ATT&CK (Sub-)Techniques
Malware	77%	94%
Ransomware	78%	92%
Web Application Hacking	86%	98%
Insider and Privilege Misuse	86%	90%
Targeted Intrusions	83%	95%

All percentages are based on ATT&CK (sub-)techniques assigned to an ATT&CK mitigation.

CIS Controls v8

Introduction: CIS Critical Security Controls

Controls V8 Implementation Groups (IGs)



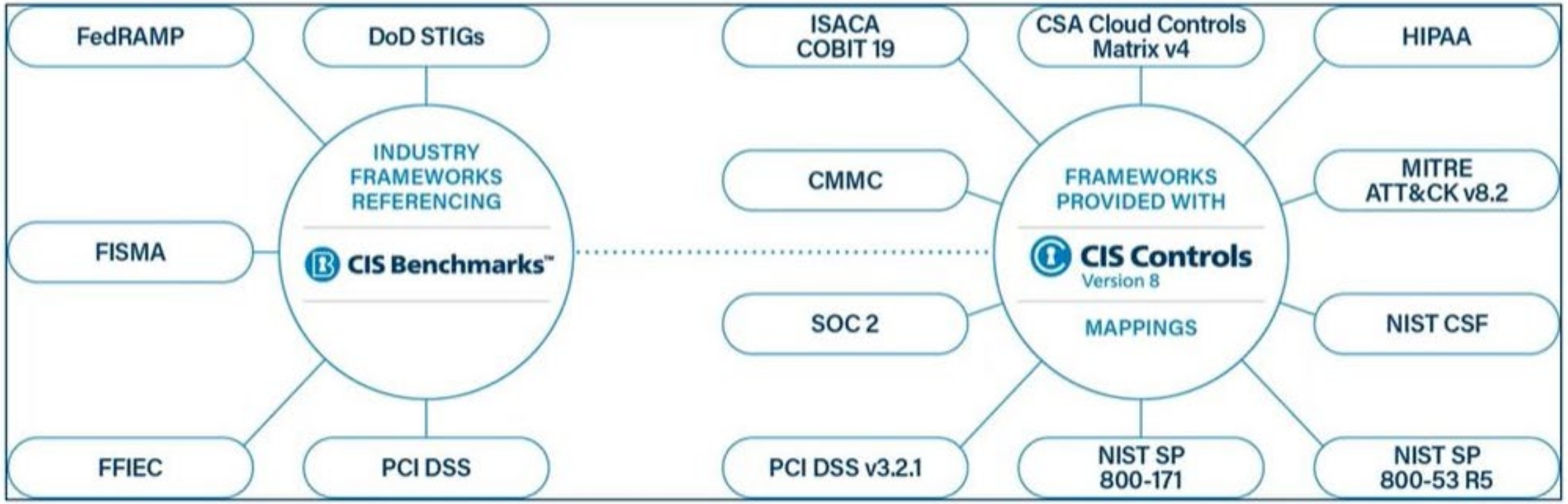
IGs are based on the risk profile and resources an enterprise has available to them to implement the CIS Controls.

Every enterprise should start with IG1, ***Essential Cyber Hygiene.***

https://www.cisecurity.org/insights/white-papers/implementation-guide-for-small-and-medium-sized-enterprises-cis-controls-ig1

Referenced by Industry Standards

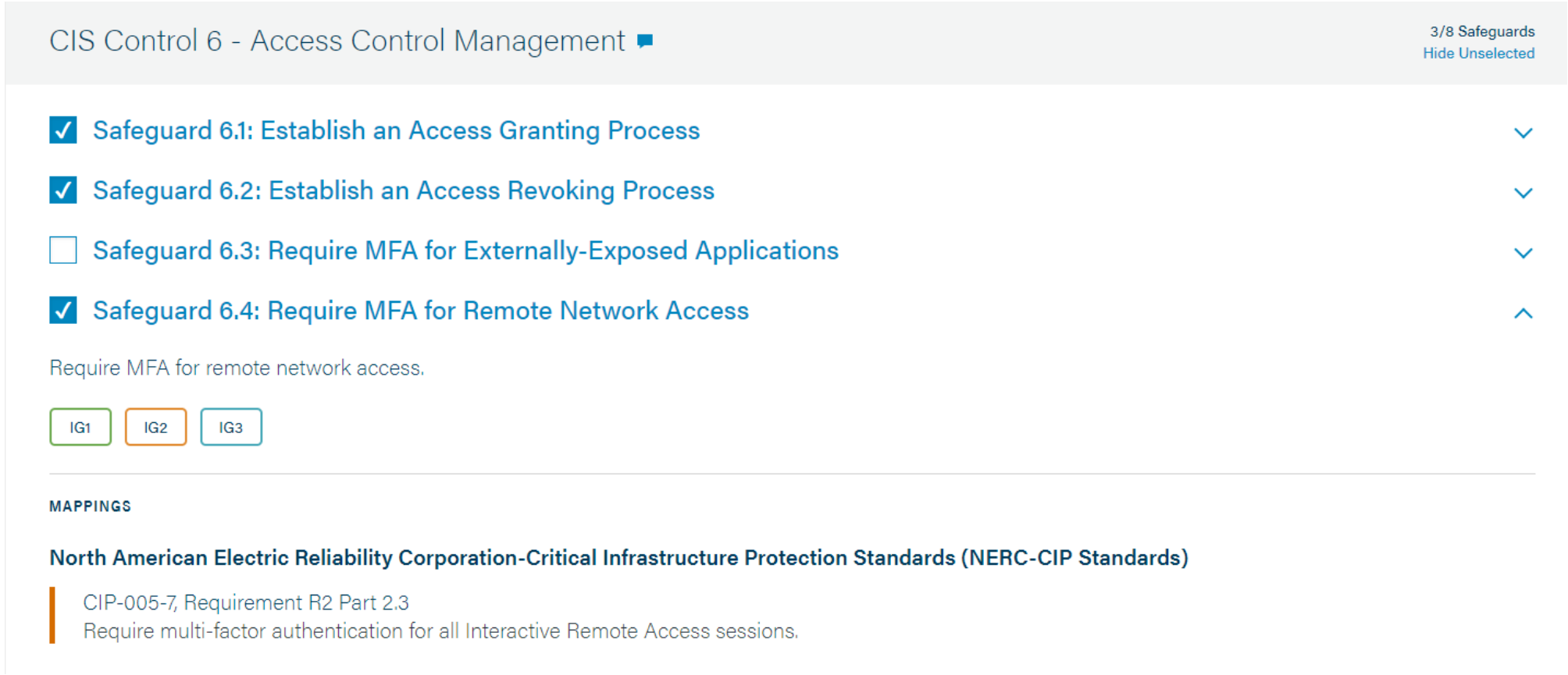
Assisting Organizations That are Working Towards Compliance



Controls Navigator Tool

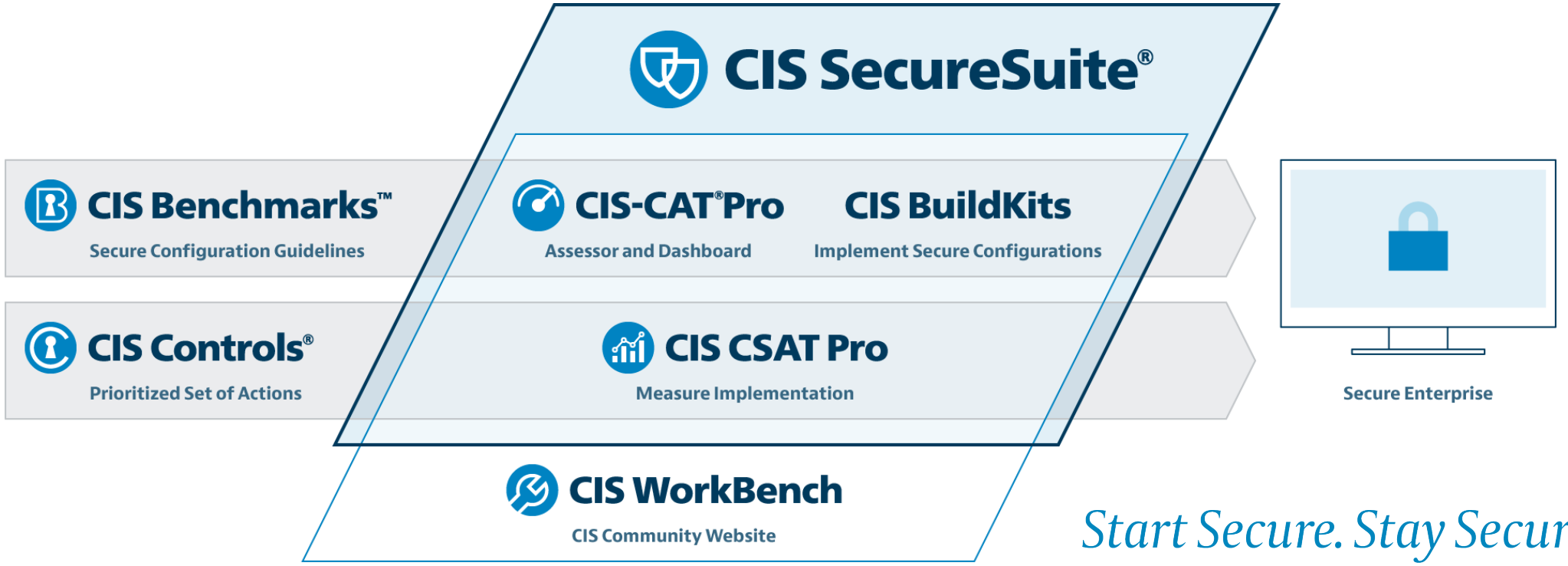
https://www.cisecurity.org/controls/cis-controls-navigator

- Explore how the Controls map to your broader security program
- Broken down by Implementation Group



CIS SecureSuite®

FreeSecureSuite@cisecurity.org

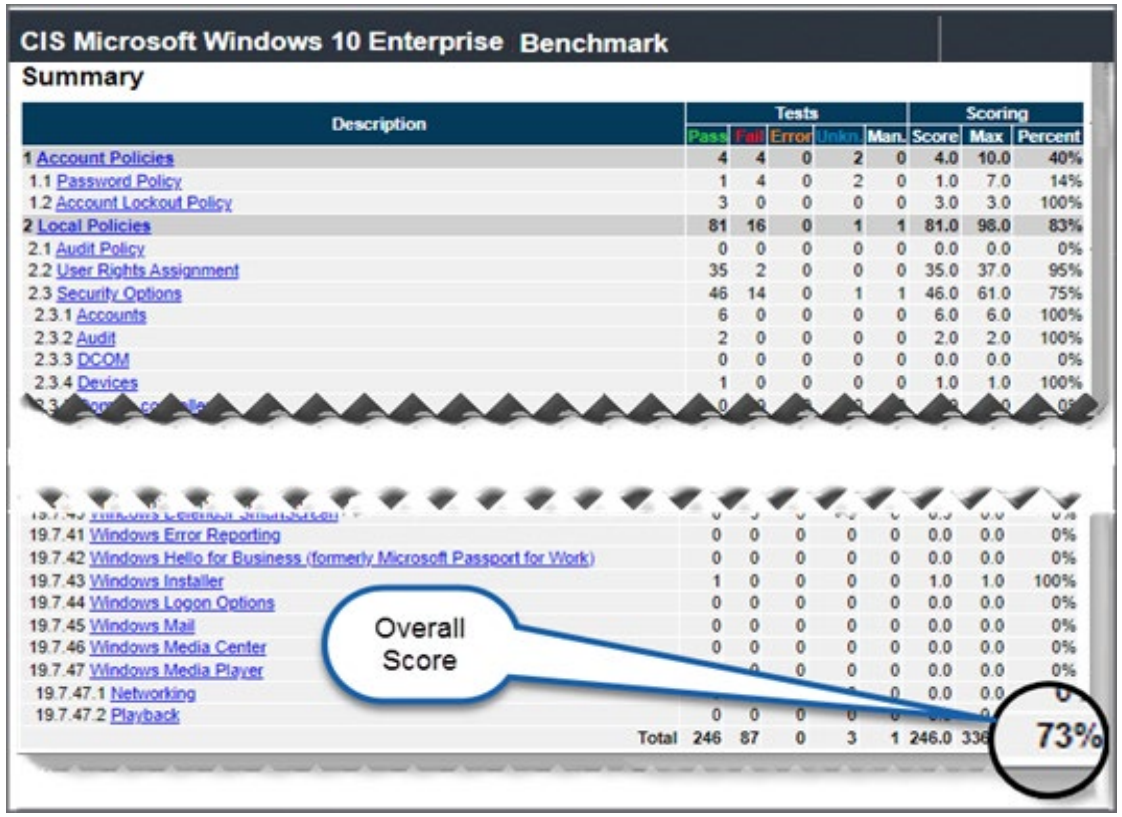


https://www.cisecurity.org/cis-securesuite/member-webinars

CIS-CAT Actionable Results

Configuration Result Output

- **Organization cyber security policy will dictate accepted score**
- **Out of the box systems** score **< 30%**
- **Aim for a score between 85%-95%**
- CIS-CAT® Pro Assessor evaluates the cybersecurity posture (**configuration**) of a system against recommended configuration policy settings (**CIS Benchmarks**).



Nationwide Cybersecurity Review (NCSR)

- Annual, self-Assessment
- NIST Framework
- Cybersecurity Roadmap

For More Information:

https://www.cisecurity.org/ms-isac/services/ncsr

- **2024 NCSR**
  - Currently CLOSED for Registration
  - Registration Opens October 1st
- **Registration & Resources**
  - Located on NCSR Webpage
  - End-User Guidance
  - Results & Reporting Templates

https://www.cisecurity.org/insights/white-papers/2022-nationwide-cybersecurity-review

Best Practice Resources

NCSR Resources

Metrics Working Group Reference Guides

- Using Cybersecurity Metrics to Inform Stakeholders
- NCSR Data Reporting Template
- NIST CSF Policy Template Guide
- Cybersecurity Resources Guide
- Supply Chain Cybersecurity Resources Guide
- First Steps in Establishing Essential Cyber Hygiene
- Risk Assessment Guide
- The NCSR & Your HIPAA Security Rule Assessment

To join the Metrics Working Group, reach out to ncsr@cisecurity.org.

Malicious Domain Blocking and Reporting (MDBR)

https://mdbr.cisecurity.org/

Security Focused DNS service:

Blocks malicious domain requests before a connection is even established!

Simple Implementation:

No new hardware or software required

Helps limit infections related to:

- Known Malware
- Ransomware
- Phishing
- Other cyber threats

Security Operations Center

24x7x365

Support

Network Monitoring Services + Research and Analysis

Analysis & Monitoring

Threats, Vulnerabilities + Attacks

Reporting

Cyber Alerts & Advisories

Web Defacements

Account Compromises

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org

Cyber Incident Response Team (CIRT)

- Incident Response
- Malware Analysis
- Log Analysis

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org

No-Cost MS-ISAC Benefits to SLTTs

https://learn.cisecurity.org/ms-isac-registration

Cyber Threat Intelligence

- Cyber Alerts & Advisories
- Quarterly Threat Report
- Regular Indicators of Compromise (IOCs)
- White Papers
- Cyber Threat Briefings
- Real-Time Intelligence Feeds

Cybersecurity Services

- 24x7x365 Security Operations Center (SOC)
- Cyber Incident Response Team (CIRT)
- ISAC Threat Notification Service (IP & Domain Monitoring)
- Malicious Domain Blocking & Reporting (MDBR)

Cyber Framework & Best Practices

- Nationwide Cybersecurity Review (NCSR)
- CIS SecureSuite Membership
  - *Tools to implement the CIS Critical Security Controls and CIS Benchmarks*

Other Member Resources

- MS-ISAC Webinars
- MS-ISAC Working Groups
- CIS CyberMarket
- Virtual Service Reviews
- Homeland Security Information Network (HSIN)

CISA Cyber Hygiene Program

How to Enroll

- Request your initial assessment with CISA at vulnerability@cisa.dhs.gov
- Complete the Service Request form along with other required legal documents
- Complete the Data Sharing Form
- Elect to share your reports with the MS/EI-ISAC

CISA Region 4 Chief of Cybersecurity

Sean McCloskey
sean.mccloskey@hq.dhs.gov

ANY QUESTIONS?

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Thank You!

Megan Incerto

Regional Engagement Manager, MS-ISAC

Megan.Incerto@cisecurity.org | 518-640-3655