CYBERSECURITY SERVICES FOR BUILDING CYBER RESILIENCE

Rob Main, CGCIO
Cybersecurity State Coordinator (NC)
US Department of Homeland Security
Cybersecurity and Infrastructure Security Agency – Region IV

Anthony E. Carbone, CISSP-ISSEP, CEH, CGRC
Cybersecurity Advisor (South Carolina)
US Department of Homeland Security
Cybersecurity and Infrastructure Security Agency – Region IV

TLP: GREEN

INTRODUCTION

Rob Main

- 34+ years of experience in Information Technology and Cybersecurity
- Certified Government Chief Information Officer – UNC-CH
- Masters of Business Administration – ECU
- Bachelor of Computer Science Degree – Troy University
- 25-year military veteran (USAF and NC Air National Guard)

INTRODUCTION

Anthony E. Carbone

- 38+ Years IT/Crypto/COMSEC/Cybersecurity Experience
  - 22 Years U.S. Air Force (Retired)
  - 4 Years Command Information Assurance Manager (C-IAM) – SPAWAR-SSC Charleston
  - 11 Years Special Agent – Defense Counterintelligence & Security Agency (DCSA)
- Masters of Science in Telecommunications Management – Golden Gate University
- Bachelor of Science in Information Systems Management – University of Maryland University College (UMUC)
- Certified Risk Management Framework (RMF) Security Control Assessor (SCA) & Fully Qualified U.S. Navy RMF Certifier
- Certified Ethical Hacker & Governance, Risk and Compliance (CEH/CGRC)
- Certified Enterprise Risk Professional & Independent Assessor (CERP/CEIA)

Agenda

- Introduction and Mission
- Coordinators and Advisors
- Cyber Risk Management and Operational Resilience
- CISA Cyber Services and Assessments
- Information Sharing
- Additional Resources
- Q & A

CISA
CYBER+INFRASTRUCTURE

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

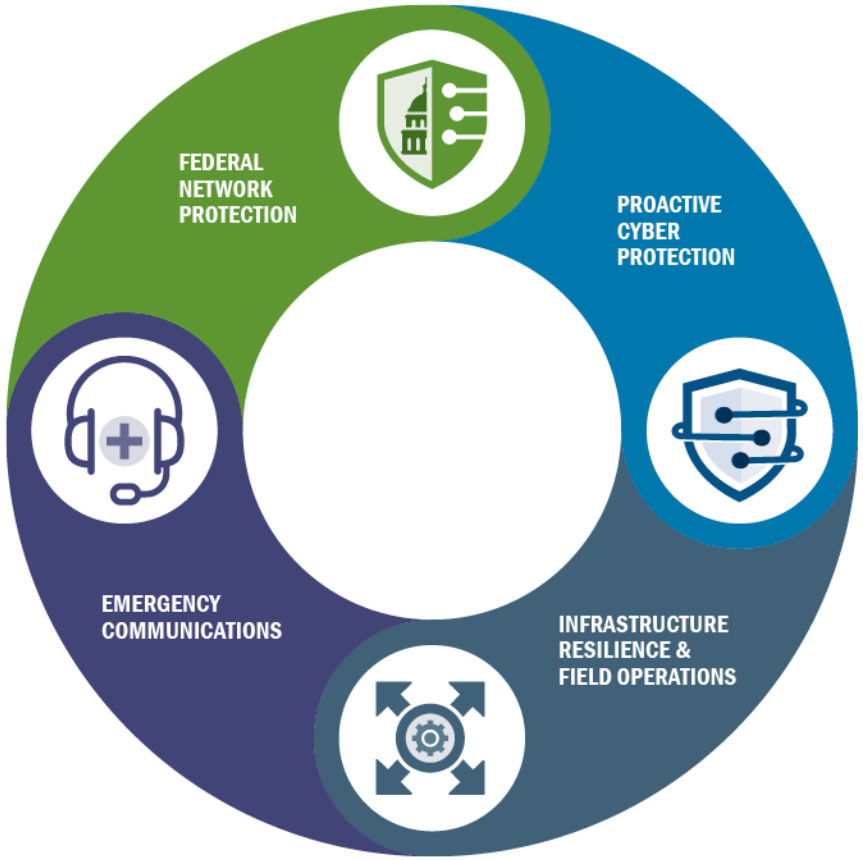
Strengthen critical infrastructure and address long-term risks

months | years | decades

TLP: GREEN

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

The Nation's Risk Managers



The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) works with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future

TLP: GREEN

Divisions of CISA

CYBERSECURITY DIVISION

INTEGRATED OPERATIONS DIVISION

INFRASTRUCTURE SECURITY DIVISION

NATIONAL RISK MANAGEMENT CENTER

EMERGENCY COMMUNICATIONS DIVISION

STAKEHOLDER ENGAGEMENT DIVISION

CISA CYBER+INFRASTRUCTURE

TLP: GREEN

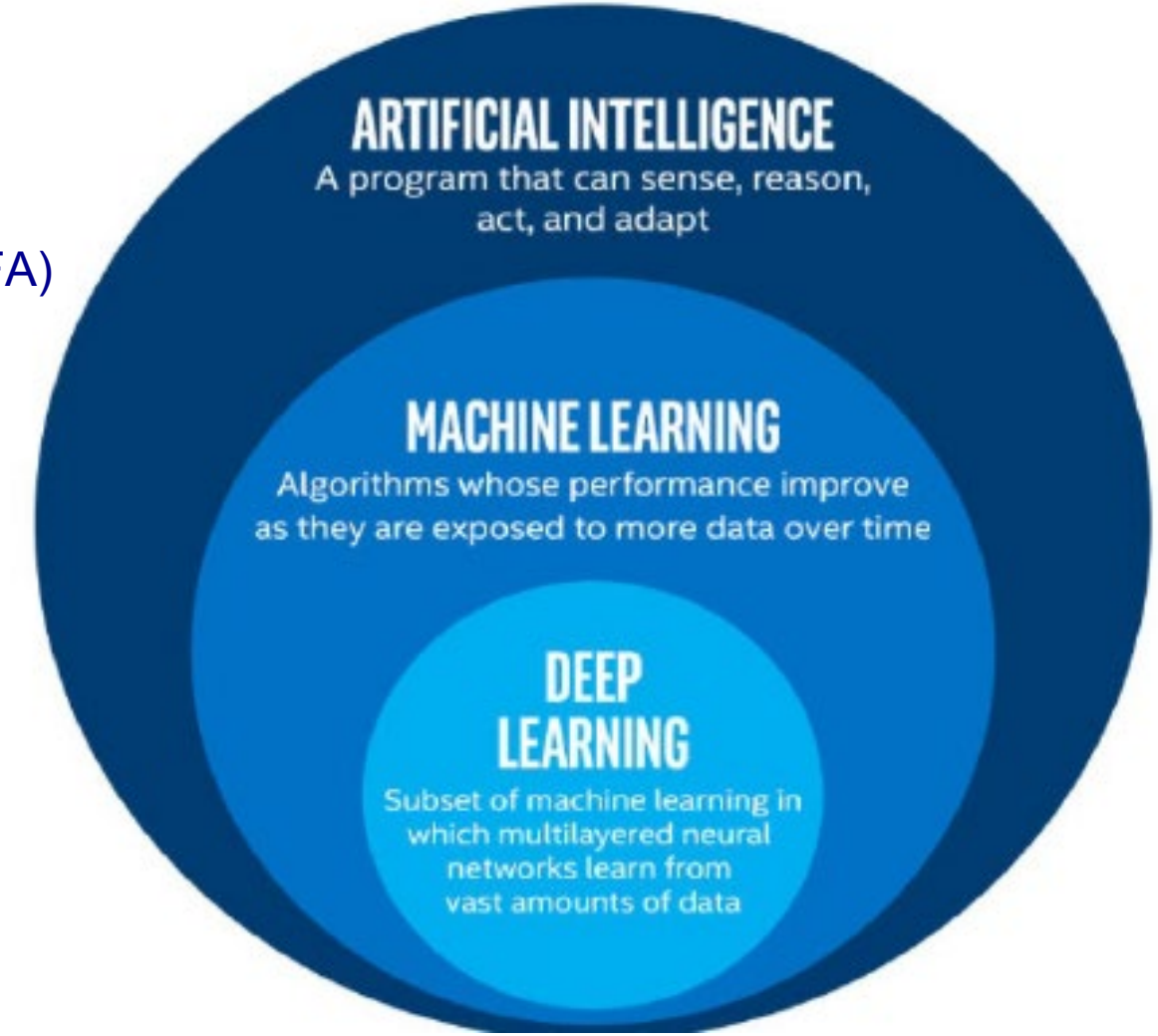
Today's Risk Landscape

America remains at risk from a variety of threats:

TLP: GREEN

Advanced Threats

- **Social Engineering**
  - Scattered Spider (aka – Starfraud & UNC3944)
    - SIM Swapping
    - Account Takeovers (Reset Passwords, remove MFA)
    - Data Exfiltration, Extortion, Ransomware
- **Artificial Intelligence (AI)**
  - Machine Learning
  - Neural Networks
  - Large Language Models
  - Generative AI
    - Deep Fakes



CISA CYBER+INFRASTRUCTURE

TLP: GREEN

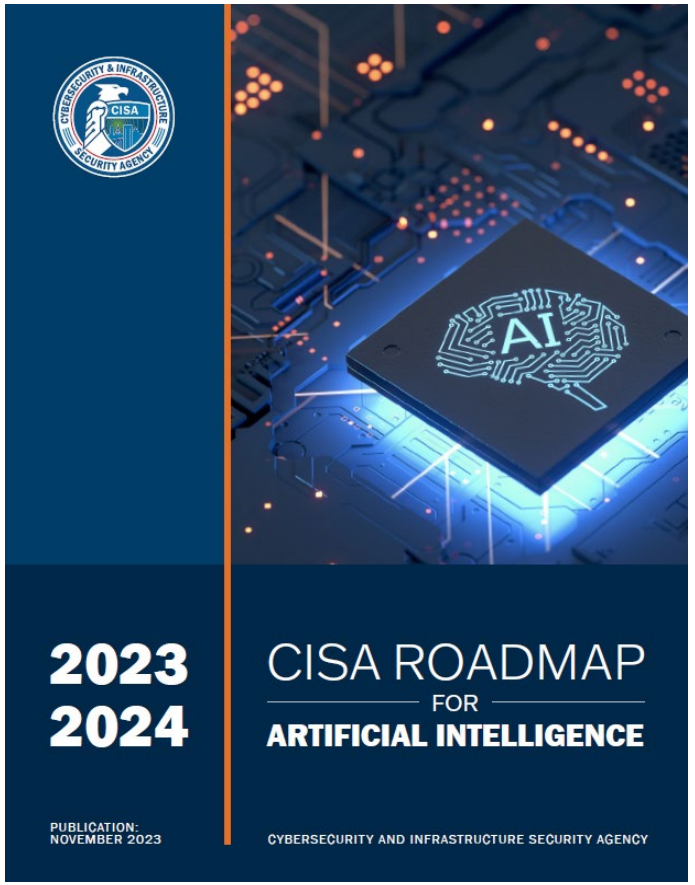
Roadmap for Artificial Intelligence

Purpose

CISA's AI Roadmap is a whole-of-agency plan aligned with national AI strategy to align our cross-agency efforts and communicate our role in AI safety and security.

Areas of Focus

1. Promote the beneficial uses of AI to **enhance cybersecurity capabilities**.
2. Ensure **AI systems are protected from cyber-based threats**.
3. **Deter the malicious use of AI capabilities** to threaten the critical infrastructure Americans rely on every day.



CISA
CYBER+INFRASTRUCTURE

TLP: GREEN

Quantum Computing and Artificial Intelligence

What is Quantum Computing?

- Rapidly evolving field which harnesses the unique qualities of quantum mechanics to solve the most complex problems beyond the capabilities of classical computing

Cryptographically Relevant Quantum Computer (CRQC):

- Small, laboratory-scale examples have been built
- Capable of undermining public key algorithms used for asymmetric key exchanges & digital signatures
- Pre-shared keys *may* mitigate the threat

CRQC and AI Opportunities:

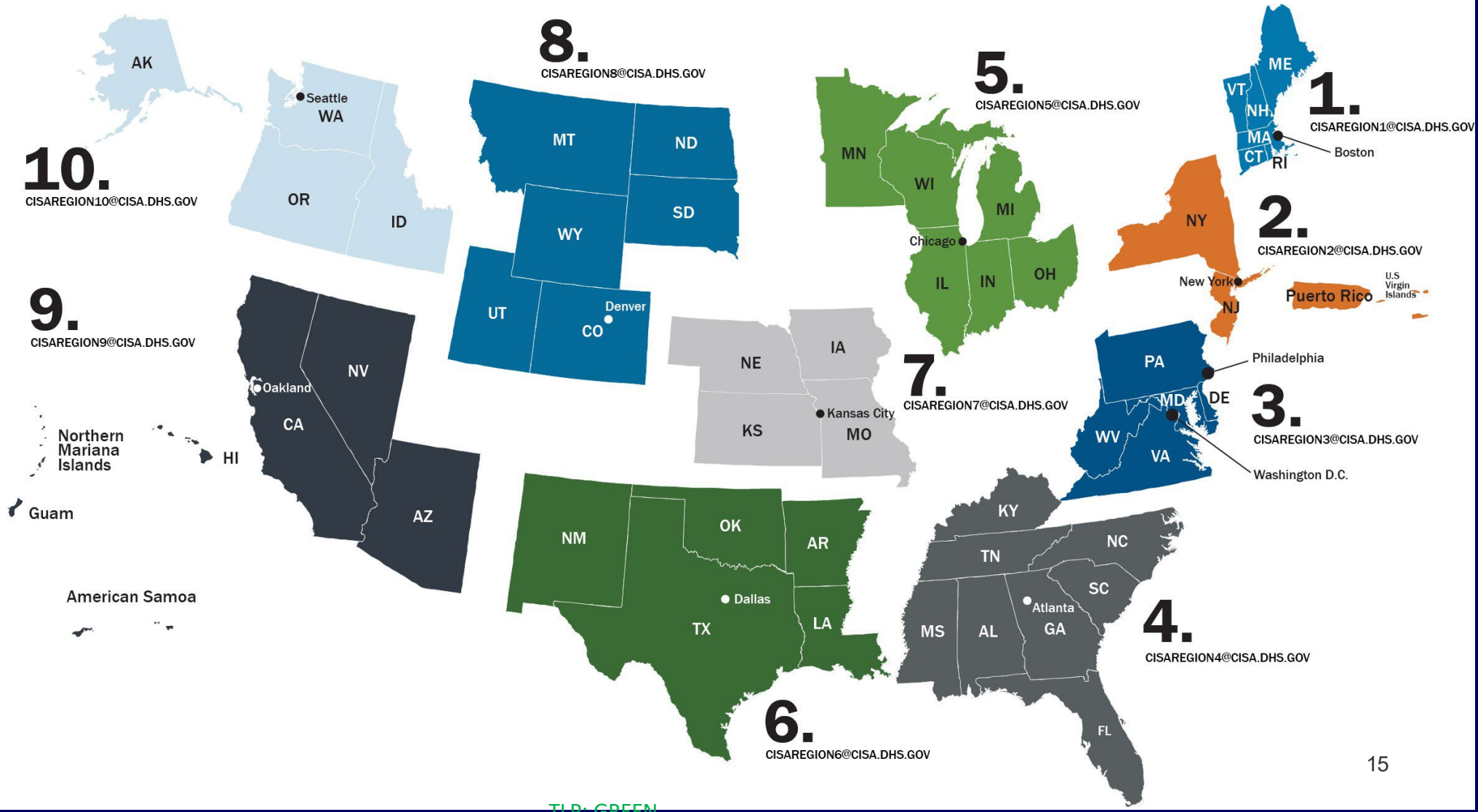
- Reduce training data needed for LLM
- Reduce training time needed for LLM
- Increase capabilities of LLM

CRQC and AI Risks:

- Training data manipulation
- Exploitation of algorithmic vulnerabilities
- De-anonymization of private data
- Malicious content generation

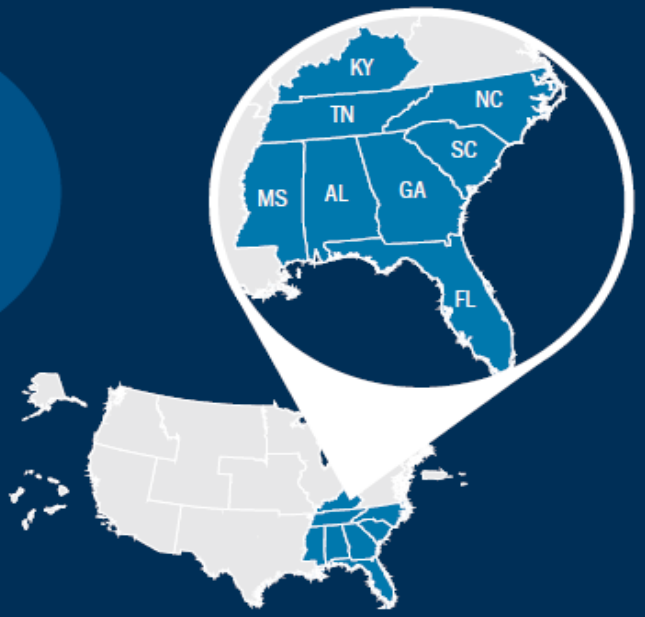
CISA Regions

1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Dallas, TX
7	Kansas City, MO
8	Denver, CO
9	Oakland, CA
10	Seattle, WA



TLP: GREEN

CISA
CYBER+INFRASTRUCTURE



CYBERSECURITY + INFRASTRUCTURE SECURITY AGENCY

REGION IV

REGION IV AT-A-GLANCE

REGIONAL OFFICE:
ATLANTA, GEORGIA

LOCATION:
8 STATES
6 TRIBAL NATIONS

SIZE:
394,420 SQUARE MILES

ESTIMATED POPULATION:
65.733 MILLION

KEY FACTS:

- Contains 17 nuclear power facilities (with applications for nine new sites pending). These facilities supply 29 percent of the nation's electrical power output
- Harbors six nationally critical ports
- Home to 7 of the country's fastest growing cities: Orlando, FL; Nashville, TN; Cape Coral, FL; West Palm Beach, FL; North Port, FL; Lakeland, FL; and Raleigh, NC (2018 data).

Protective Security Advisors

Protective Security Advisors (PSA) have five mission areas directly supporting the protection of critical infrastructure:

- Plan, coordinate, and conduct **physical** security surveys and assessments
- Plan and conduct outreach activities – public & private sector
- Support National Special Security Events (NSSEs) & Special Event Activity Rating (SEAR) events
- Support state and federal partners with critical infrastructure recovery post-incident
- Coordinate and support improvised explosive device awareness and risk mitigation training & assessments

Emergency Communications Coordinators

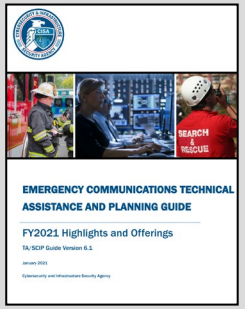
Governance

Regional Coordination

Strategic Planning

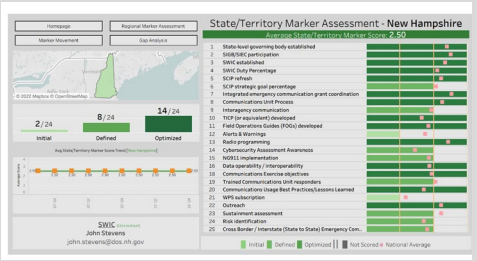
State & Tribal Communications Interoperability Plans

Technical Assistance



Service Offerings Guides

Assessments



State Markers

ECCs support emergency communications across government and critical infrastructure

STATEWIDE INTEROPERABILITY COORDINATOR (SWIC)

ECCs maintain close relationships with SWICs and public safety personnel in their regions

Special Coordination
ESF-2 | NSSE | SEAR

6,000+ Public Safety Answering Points (911)

50,000+ Radio Systems

400,000+ Cell Towers & Radio Sites

CISA CYBER+INFRASTRUCTURE

TLP: GREEN

Chemical Security Inspectors**

Chemical Security Inspectors visit chemical facilities to ensure that they meet the security requirements set forth by the **Chemical Facility Anti-Terrorism Standards (CFATS) Regulatory Security Program**. The CFATS program identifies and regulates high-risk Chemical facilities to ensure they have security measures in place to reduce the risk that certain hazardous chemicals are not weaponized by terrorists.

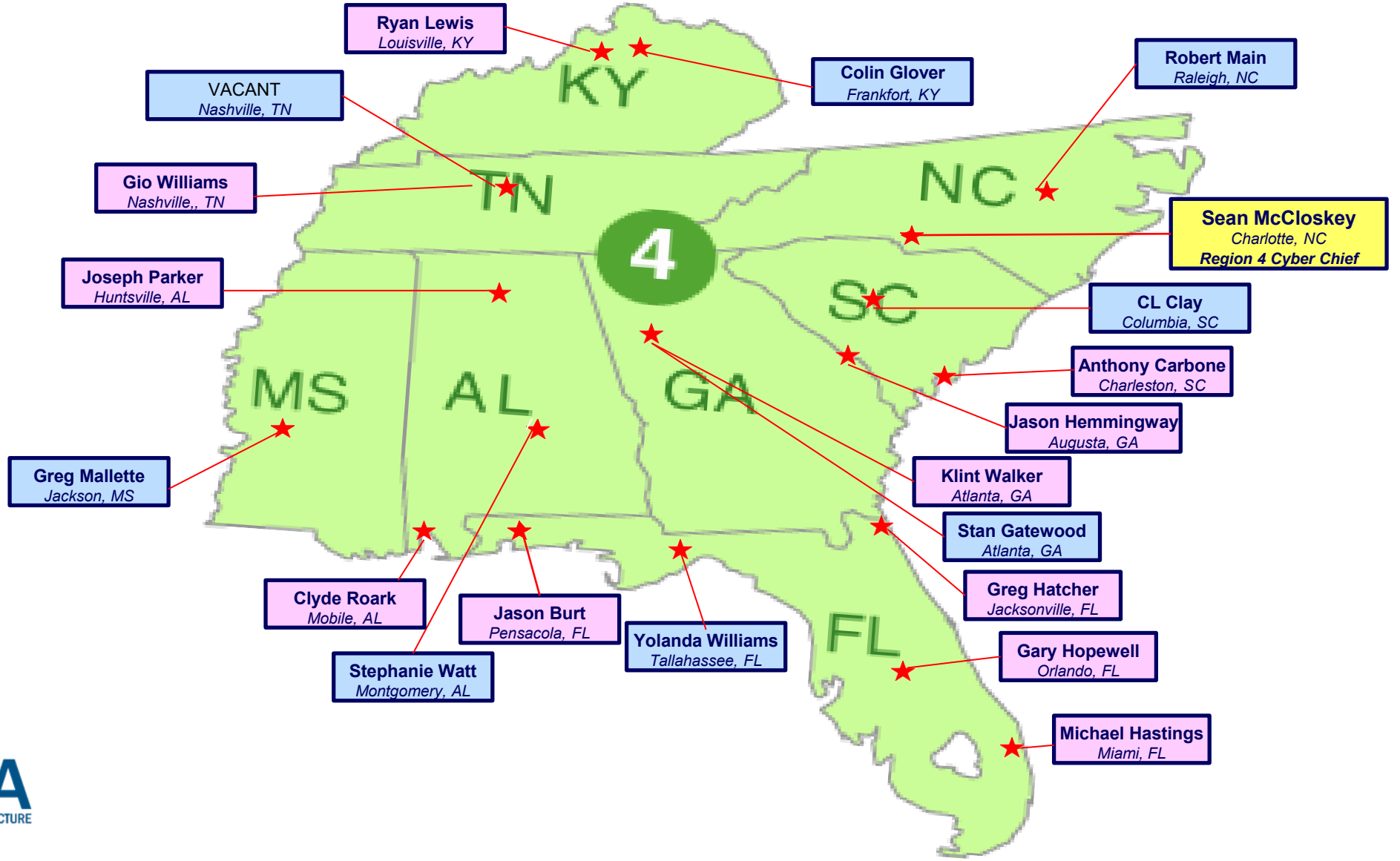
- **Plan, coordinate, and conduct regulatory Inspections and Compliance Assistance Visits**
- **Plan & Conduct Outreach engagement activities**
- **Support Enforcement Operations**
- **Support Chemical sector security events**

Election Security Advisors

- On **July 25, 2023**, Director Easterly announced the creation of these ten positions (one per region) due to the unparalleled importance of elections as a foundational component of who we are as a nation
- **Build strong connective tissue between the state and local election officials and CISA**
- **Experts in the differences in election infrastructure, jurisdiction requirements, and operating environments in their regions** so they can offer more targeted guidance and support
- **Bottom line**, doing more for election officials and are where they need ESAs to be to make that happen

CYBERSECURITY STATE COORDINATORS AND ADVISORS

CISA Region 4 Cyber Support



CISA
CYBER+INFRASTRUCTURE

CSC / CSA Lines of Effort

- **Preparedness Activities**
  - Cybersecurity Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - Information / Threat Indicator Sharing
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices

- **Response Assistance**
  - Remote / On-Site Response and Assistance
  - Incident Coordination
  - Threat intelligence and information sharing
  - Malware Analysis

- **Cybersecurity Advisors**
  - Incident response coordination
  - Cyber assessments
  - Workshops
  - Working group collaboration
  - Advisory assistance
  - Public Private Partnership Development

CISA CYBER+INFRASTRUCTURE

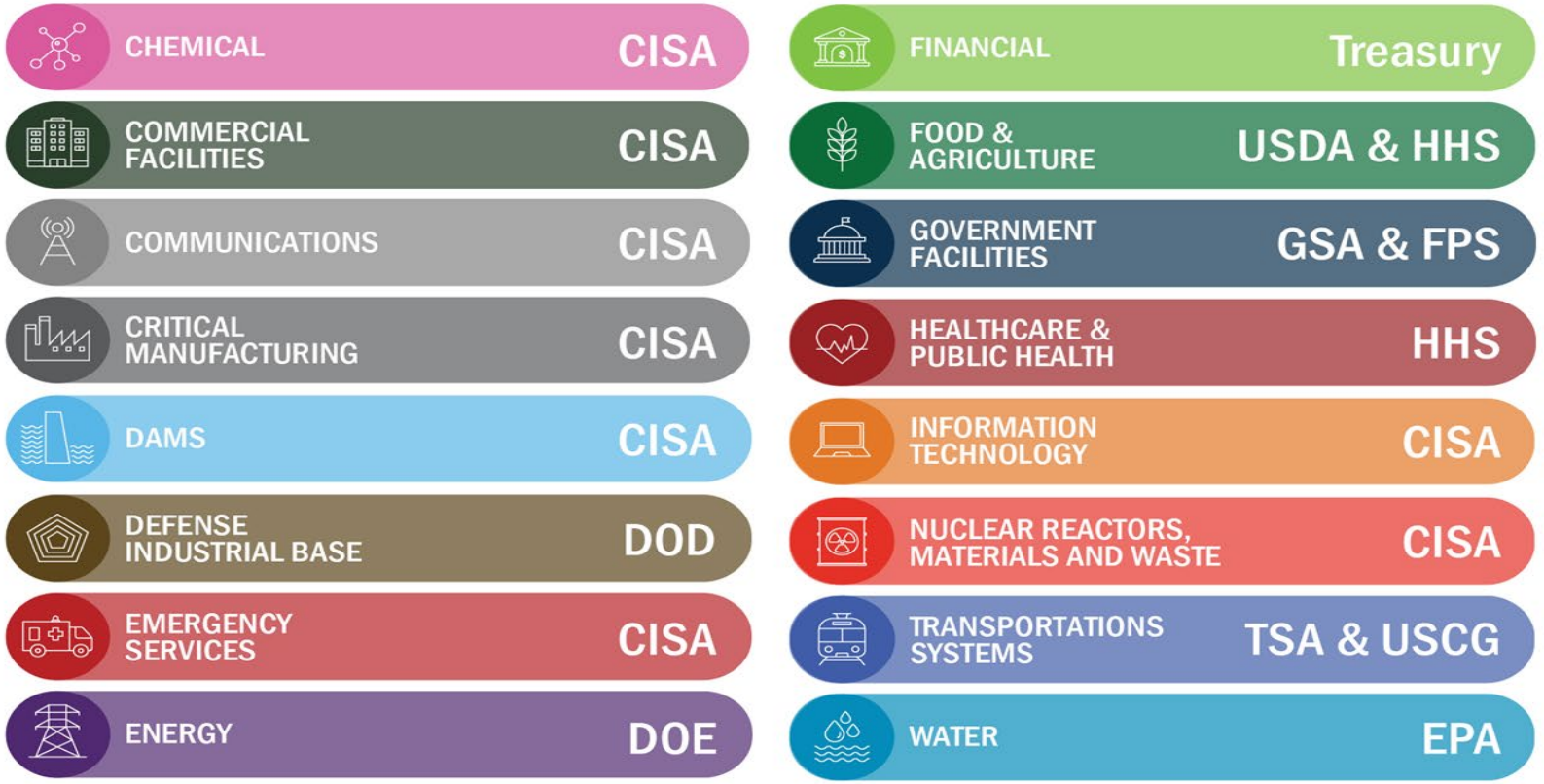
TLP: GREEN

Contact CISA to report a cyber incident

Call 1-888-282-0870 | email CISAservicedesk@cisa.dhs.gov | visit https://www.cisa.gov

Critical Infrastructure Sectors

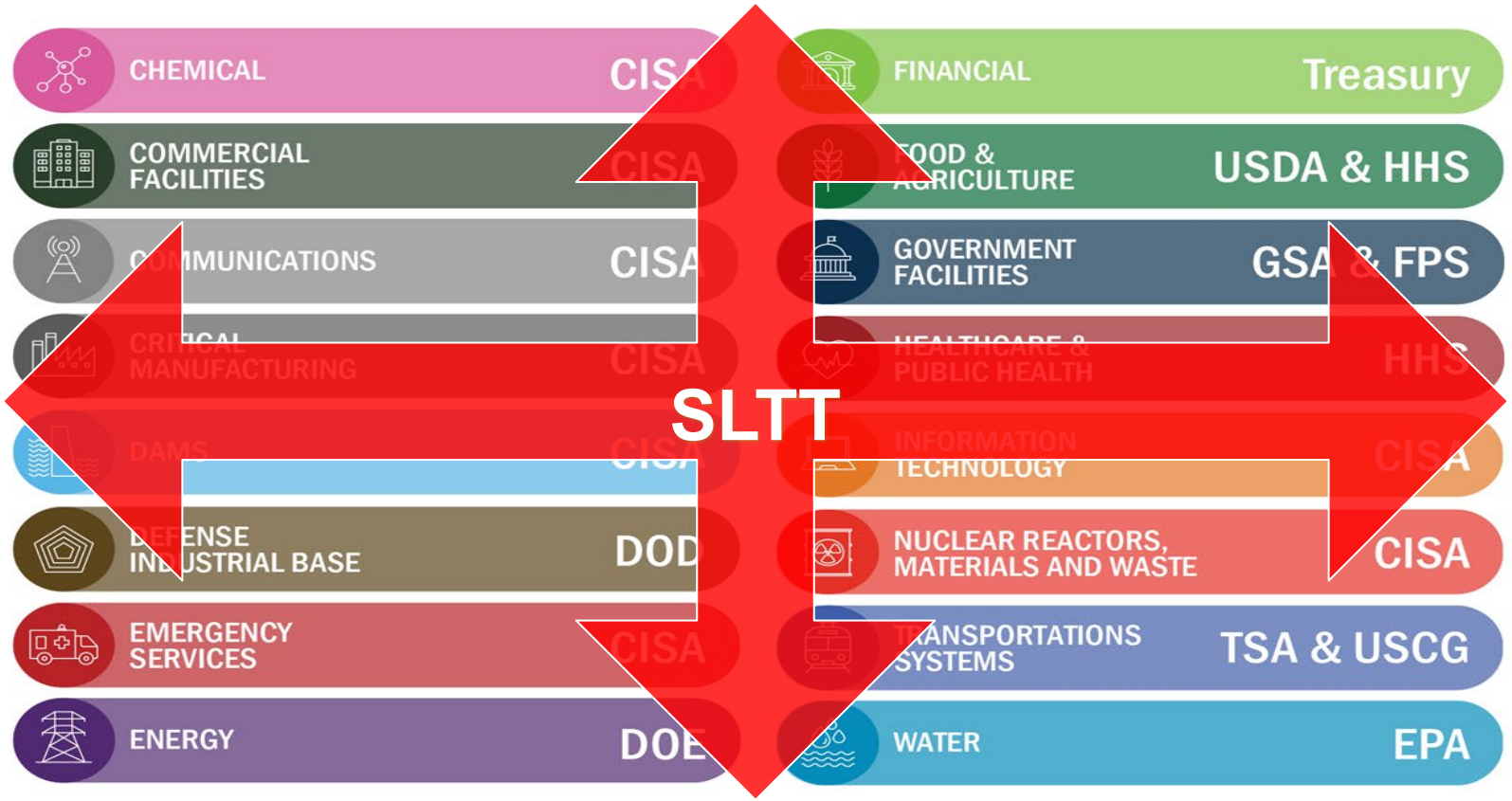
CISA assists the public and private sectors secure its networks and focuses on organizations in the following 16 critical infrastructure sectors.



CISA CYBER+INFRASTRUCTURE

TLP: GREEN

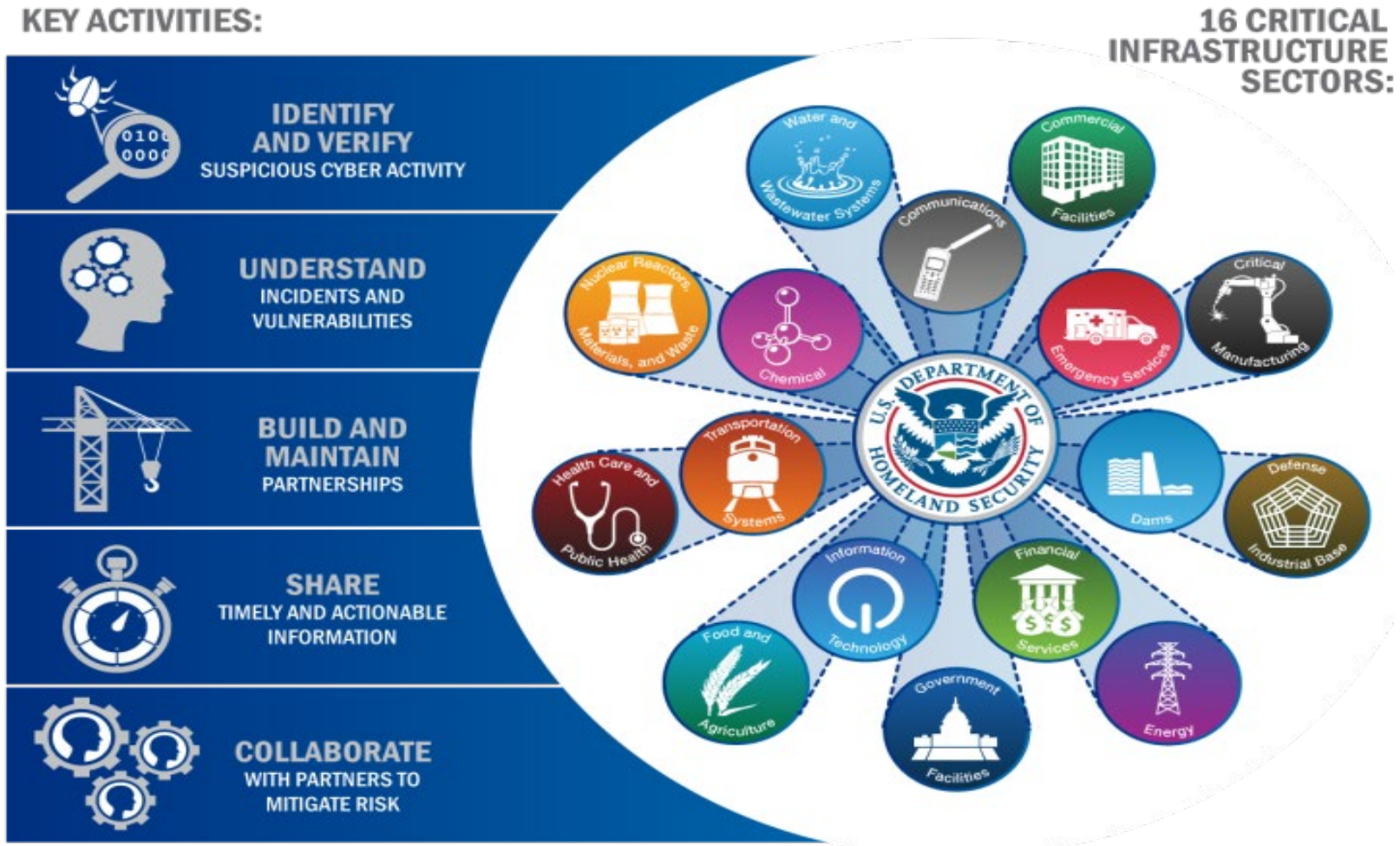
Critical Infrastructure Sectors



CISA
CYBER+INFRASTRUCTURE

TLP: GREEN

Serving Critical Infrastructure

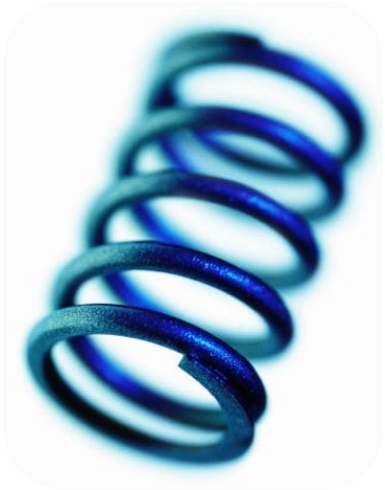


CISA
CYBER+INFRASTRUCTURE

TLP: GREEN

CYBER RISK MANAGEMENT AND OPERATIONAL RESILIENCE

What Is Resilience?



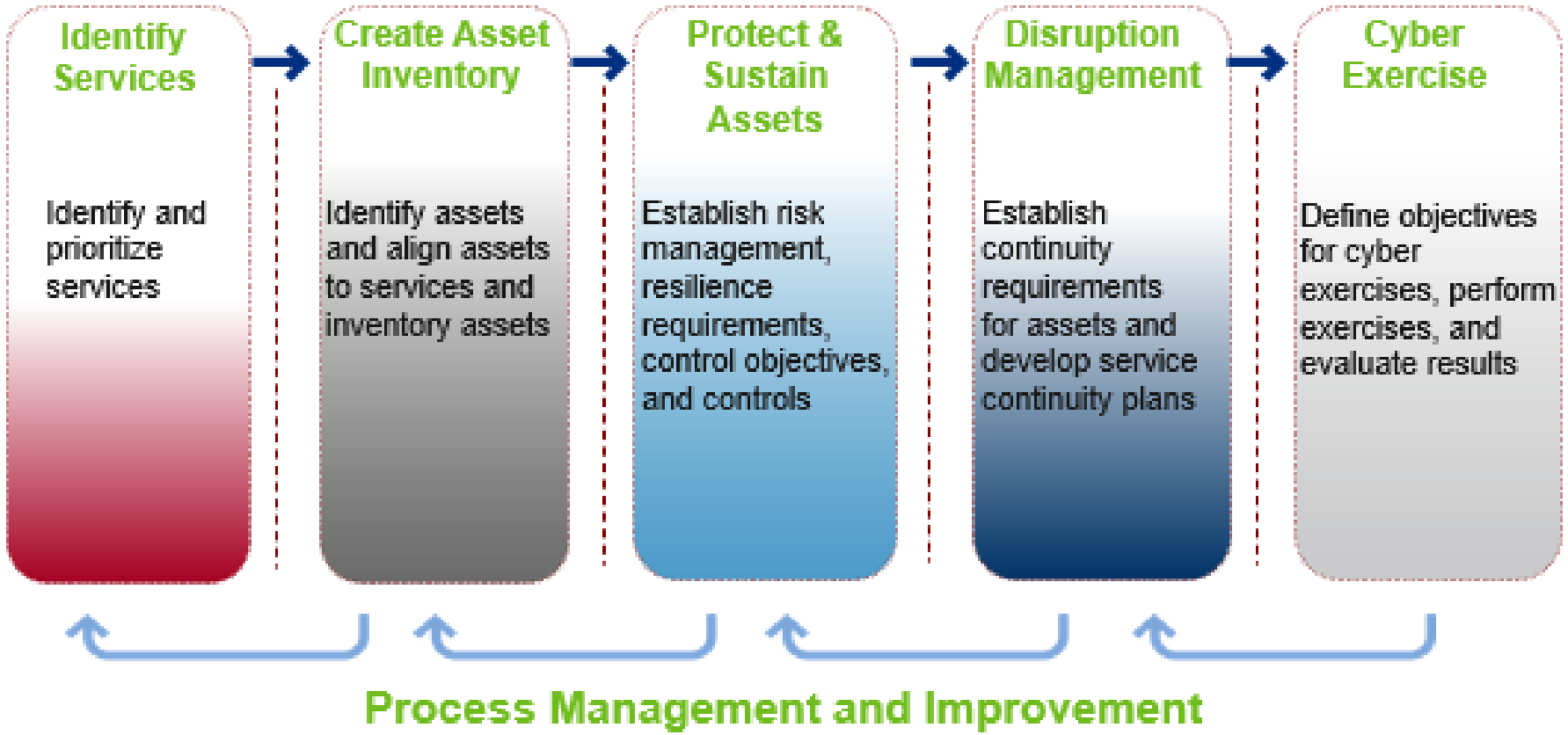
"… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"

– Presidential Policy Directive – PPD 21
Critical Infrastructure Security and Resilience
February 12, 2013

CISA
CYBER+INFRASTRUCTURE

Working Towards Cyber Resilience

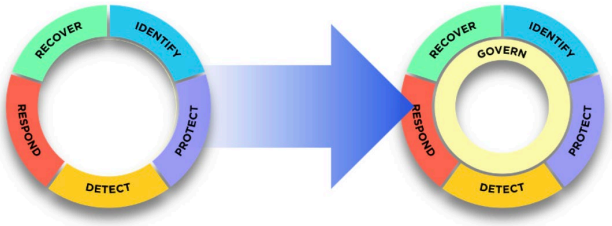
Follow a **framework** or general approach to cyber resilience.
One successful iterative approach includes:



CISA
CYBER+INFRASTRUCTURE

NIST CSF - Functions

- The Cybersecurity Framework
  - Establishes a common perspective and vernacular,
  - Provides risk-based guidelines,
  - Is collaboration-oriented, and
  - Is internationally recognized.
- For more information, visit nist.gov/cyberframework



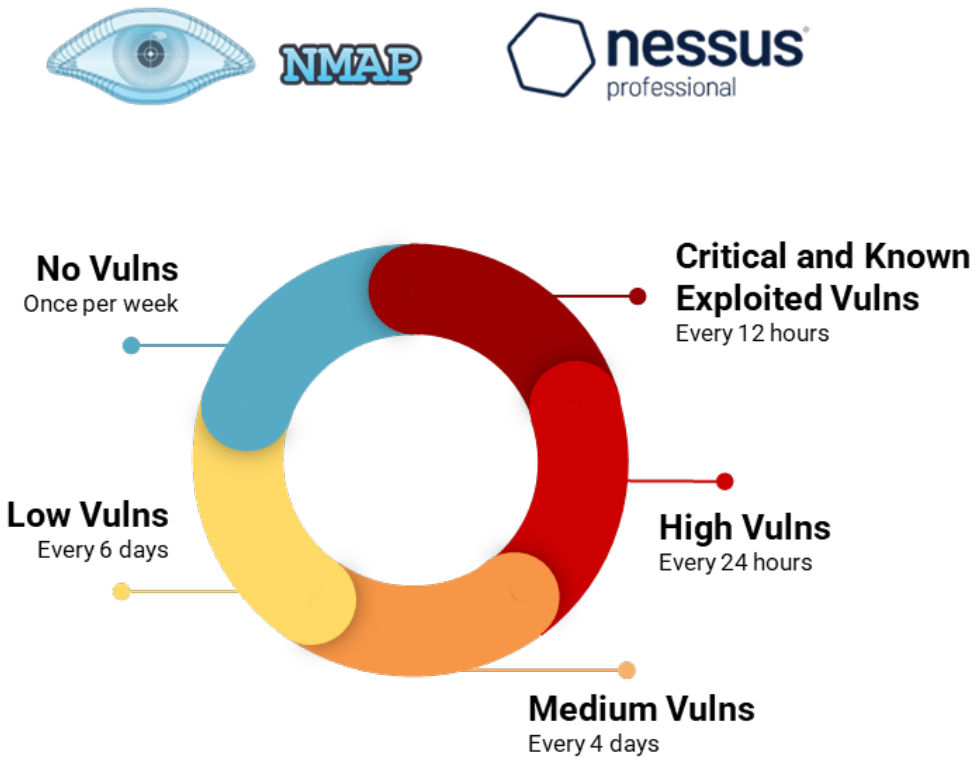
Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CISA CYBER+INFRASTRUCTURE

TLP: GREEN

CISA CYBER SERVICES

The CyHy VS Methodology



- (Nmap) – Port scanning to find open ports and listening services
- (Nessus) – Vulnerability scanning to check identified systems against a library of vulnerabilities that an Internet-based actor could exploit

Note: IPs with no open ports/listening services are port scanned only every 90 days to check for changes in host status

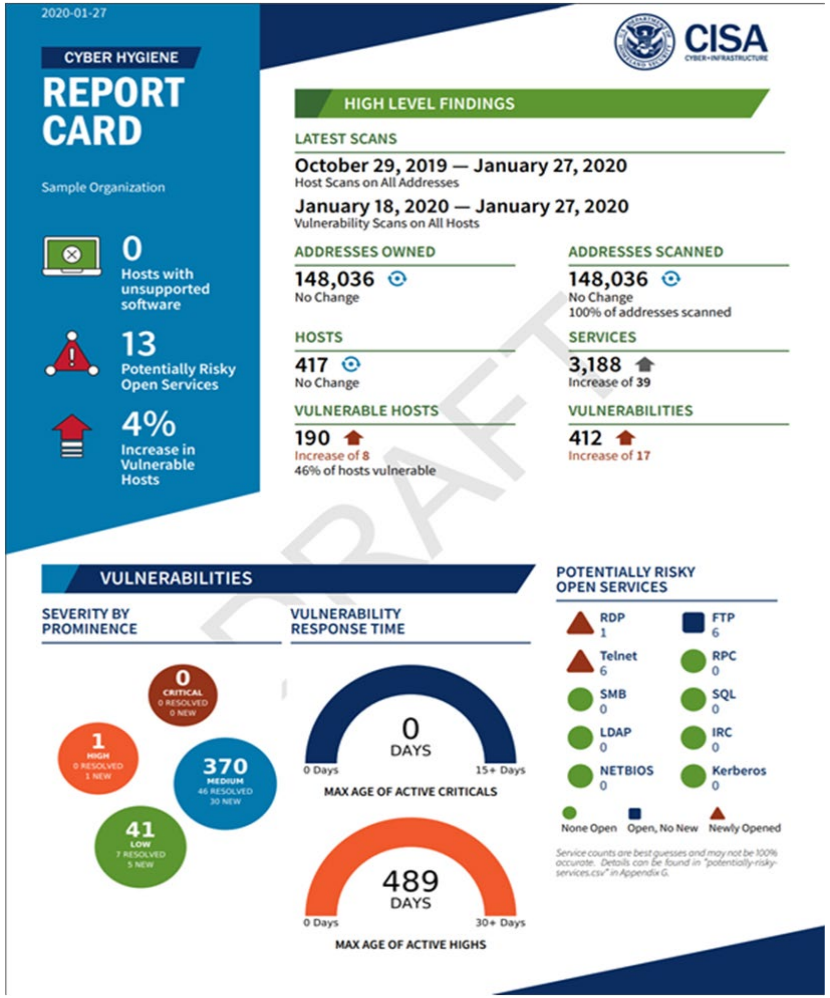
Cyber Hygiene Report Card

High Level Findings

- Latest Scans
- Addresses Owned
- Addresses Scanned
- Hosts
- Services
- Vulnerable Hosts
- Vulnerabilities

Vulnerabilities

- Severity by Prominence
- Vulnerability Response Time
- Potentially Risky Open Services



CISA CYBER+INFRASTRUCTURE

TLP: GREEN

KNOWN EXPLOITED VULNERABILITIES CATALOG

Download CSV version

Download JSON version

Download JSON schema

Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin

Back to previous page for background on known exploited vulnerabilities

Pre-Ransomware Notification Program

- Ransomware actors often take some time after gaining initial access to a target before encrypting or stealing information, a window of time that often lasts from hours to days (dwell time).
- CISA's Joint Cyber Defense Collaborative – receives tips from the cybersecurity research community, infrastructure providers, and cyber threat intelligence companies about potential early-stage ransomware activity. (report@cisa.dhs.gov)
- Local CISA field forces receive notification from our JCDC and make contact with the affected entity.
- Hundreds of notifications made weekly to Critical Infrastructure and Private Sector stakeholders:

Ransomware Vulnerability Warning Pilot (RVWP)

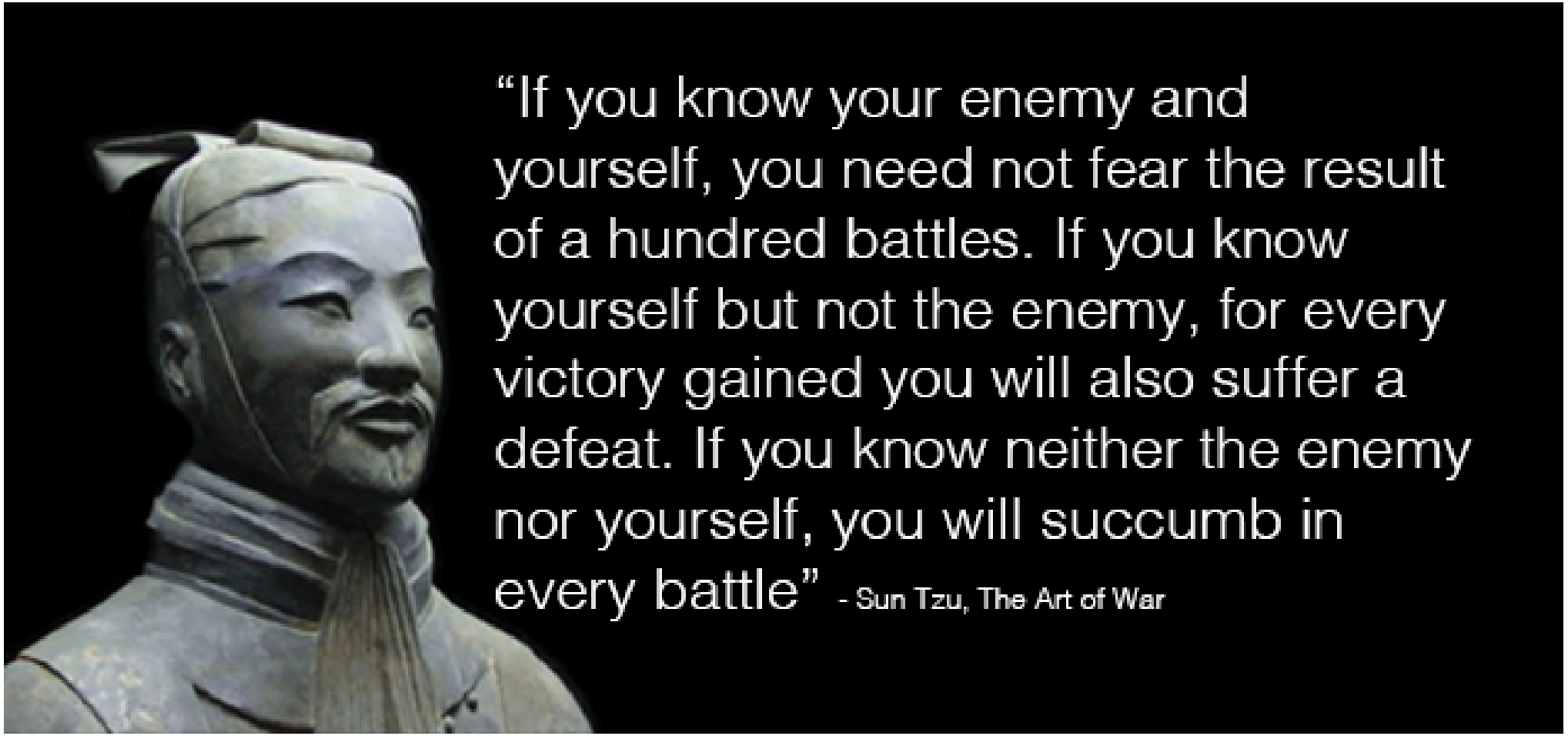
A new effort to warn critical infrastructure entities that their systems have exposed vulnerabilities that may be exploited by ransomware threat actors.

- Leverages existing authorities and technology to proactively identify information systems that contain security vulnerabilities commonly associated with ransomware attacks.
  - CISA's Cyber Hygiene Vulnerability Scanning
  - Known threat vectors
  - Administrative Subpoena Authority
  - Homeland Security Act of 2002

CISA
CYBER+INFRASTRUCTURE

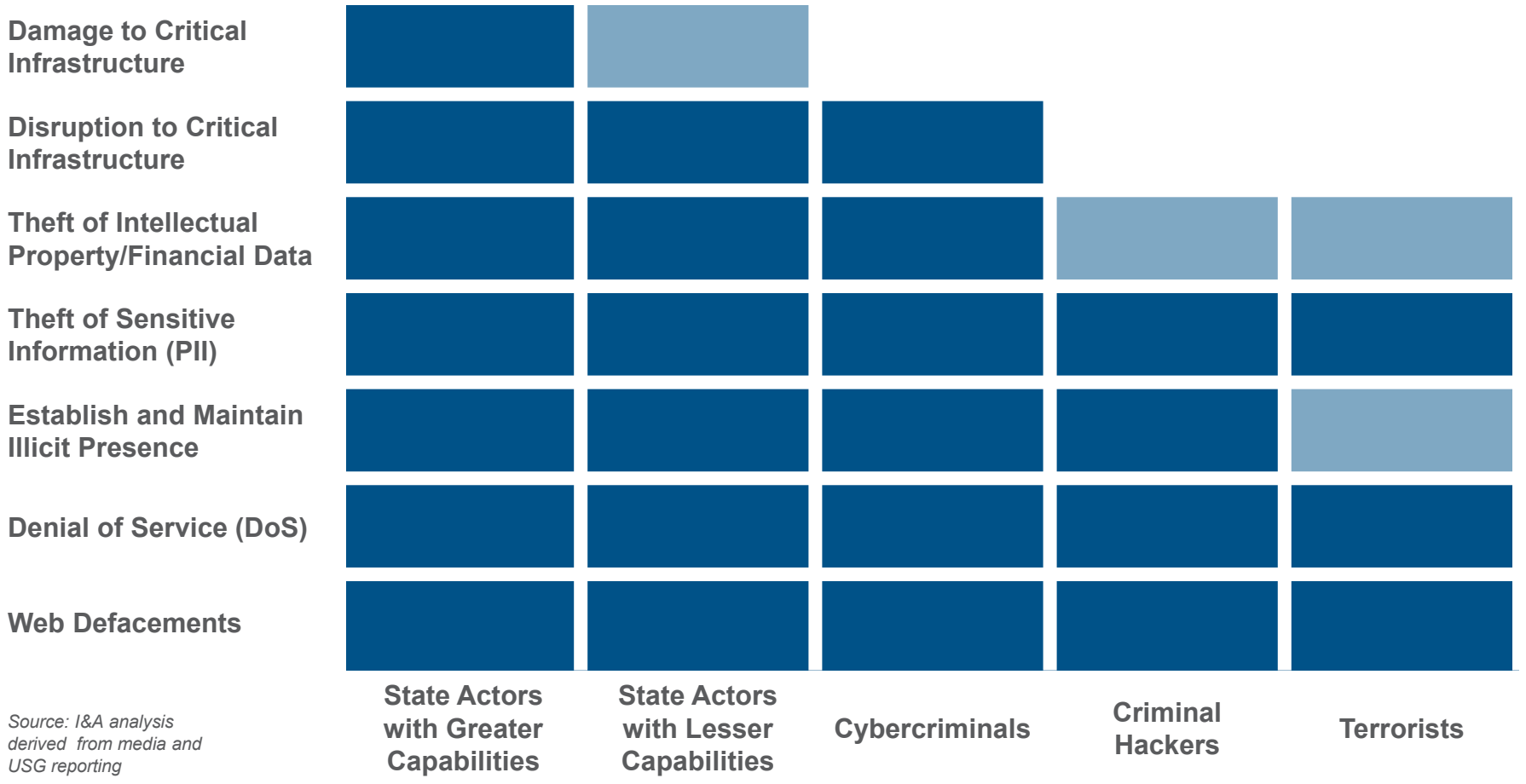
ASSESSMENTS

Know Thy Enemy



CISA
CYBER+INFRASTRUCTURE

Cyber Actor Capabilities



Source: I&A analysis derived from media and USG reporting

Note: Darker color indicates greater capability .

CISA
CYBER+INFRASTRUCTURE

Cyber Criminals

Source: DHS I&A

- **Cybercriminals**
  - Look for targets of opportunity
  - Take the path of least resistance
  - Financially motivated
  - Personal information and proprietary data: high value, high-demand commodities
- **Hacking as a service (HaaS) and Ransomware (RaaS)**
  - Malicious tools readily available for purchase or download.
  - Enable less skilled actors to effectively operate

CISA CYBER+INFRASTRUCTURE

Criticality of Periodic Assessments

Periodic Assessments Are Essential for Resilience

Can’t protect what you can’t see

Can’t fix a problem
if you don’t know what’s wrong

CISA
CYBER+INFRASTRUCTURE

Cybersecurity Resources and Assessments

Regional Resources:

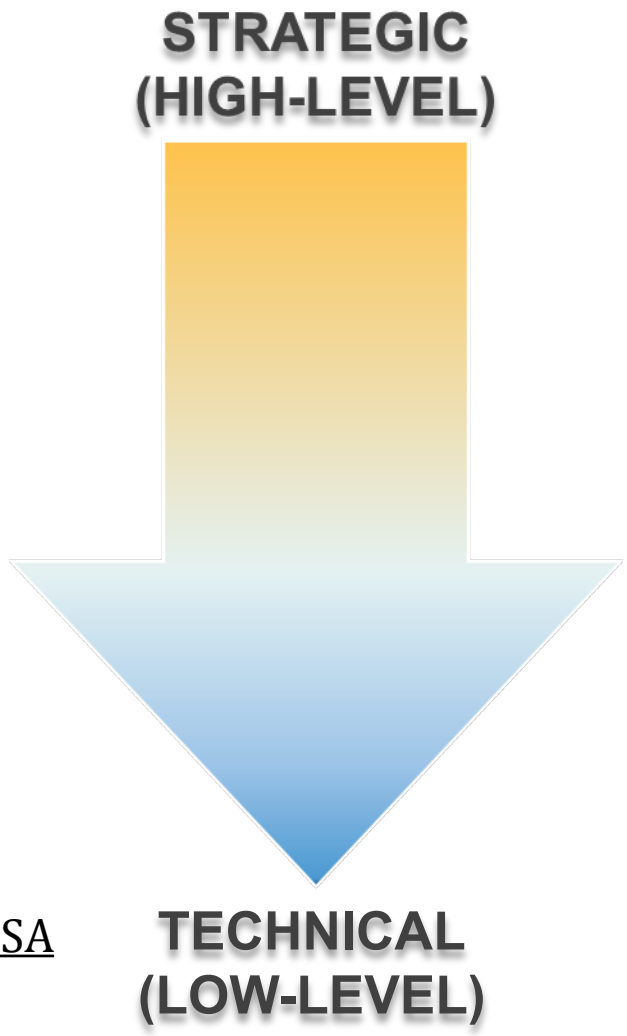
- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)
- Cyber Incident Management Review (IMR)
- Cybersecurity Performance Goals (CPG)*
- Ransomware Readiness Assessment (RRA)*
- Workshops

National Resources:

- Cyber Tabletop Exercises (CTTX)
  CTEP Package Documents | CISA
- Vulnerability Scanning Service (CyHy)

Tools:

- Downloading and Installing CSET | CISA
- Known Exploited Vulnerabilities Catalog | CISA
- Helping Cyber Defenders "Decide" to Use MITRE ATT&CK | CISA
- Untitled Goose Tool Fact Sheet | CISA (Azure)



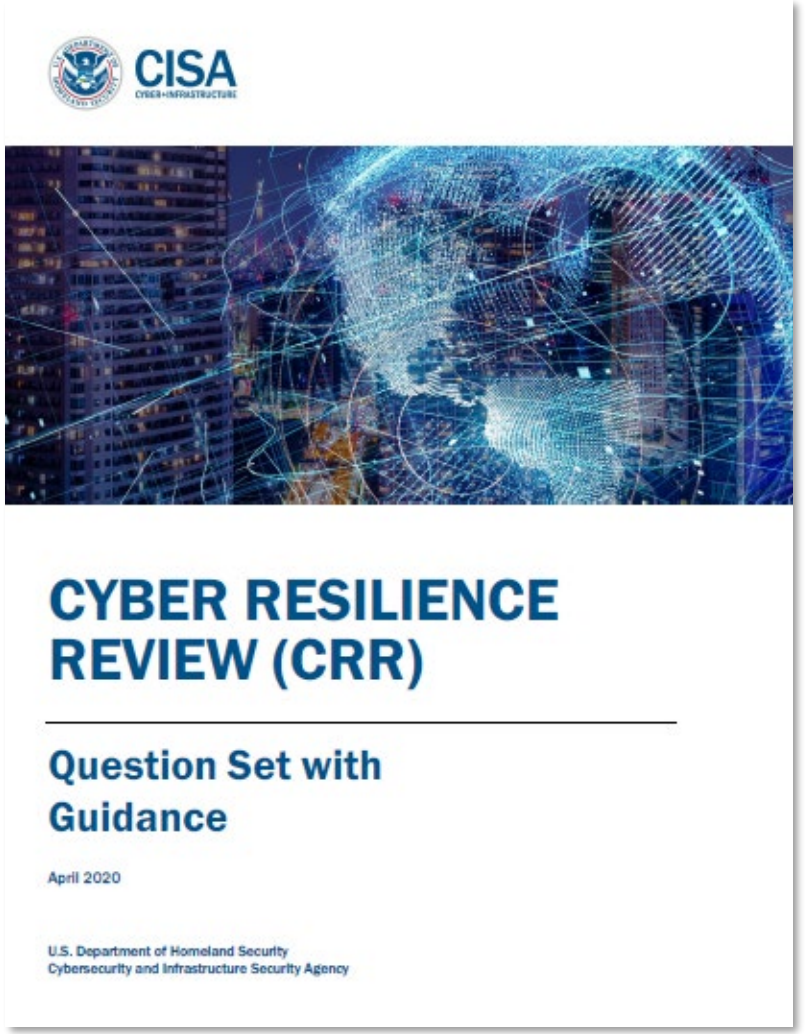
CISA CYBER+INFRASTRUCTURE

Cyber Resilience Review

- **Purpose:** Evaluates that **maturity** of an organization's capacities and capabilities in performing, planning, managing, measuring, and defining **cybersecurity capabilities** across the following 10 domains:

Asset Management	Service Continuity Management
Controls Management	Risk Management
Configuration and Change Management	External Dependency Management
Vulnerability Management	Training and Awareness
Incident Management	Situational Awareness

- **Benefits**: Helps public and private sector partners understand and measure cybersecurity capabilities as they relate to operational resilience and cyber risk



CISA CYBER+INFRASTRUCTURE

TLP: GREEN

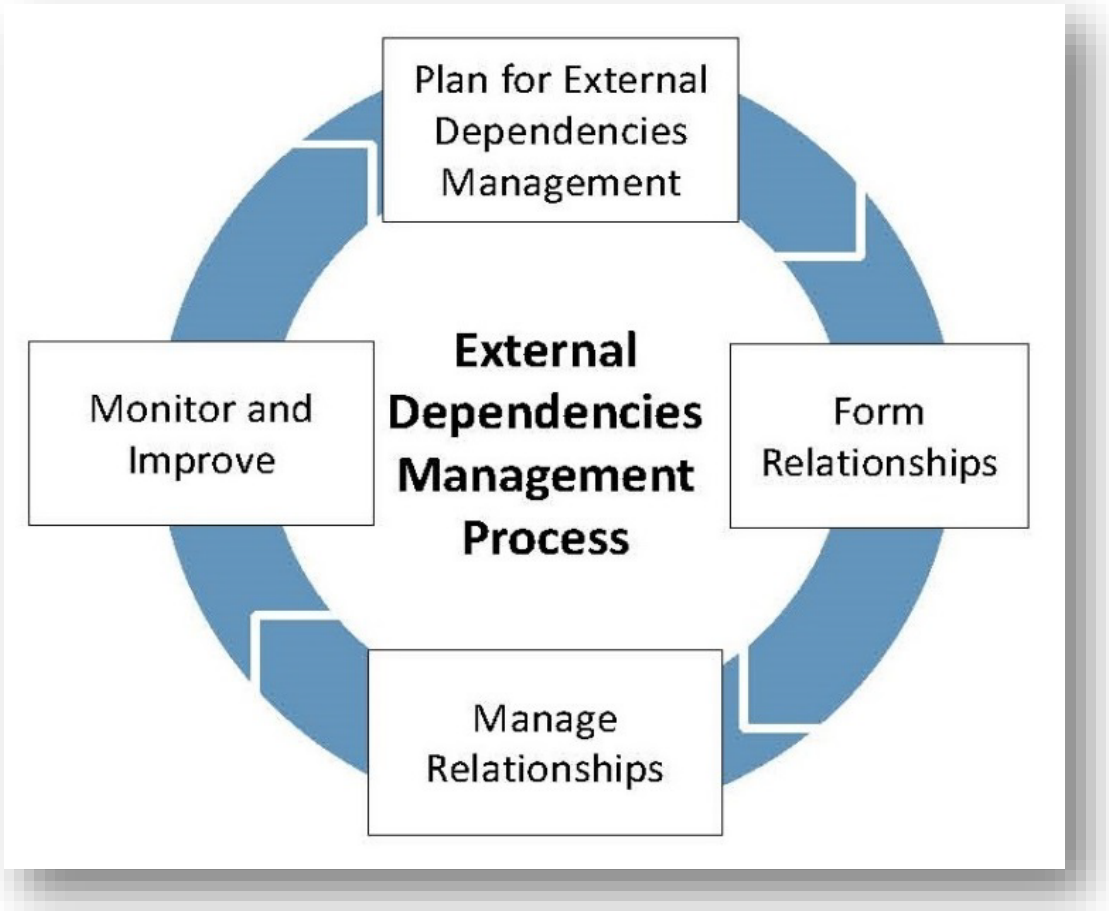
CROSS-SECTOR CYBERSECURITY PERFORMANCE GOALS

The CPGs are:

- Completely voluntary, but recommended - Applicable across all critical infrastructure sectors
- A prioritized subset of IT and operational technology (OT) cybersecurity practices to meaningfully reduce the likelihood and impact of known risks and adversary techniques
- Informed by threats observed by **CISA and its government and industry partners**
- Not Comprehensive But Very Good Starting Point – Does Not identify all cybersecurity practices to protect national and economic security and public health/safety, but captures core practices

External Dependencies Management Assessment

- **Purpose:** Evaluate an entity's management of their dependencies on third-party entities
- **Delivery:** CSC/CSA-facilitated
- **Benefits**:
  - Better understanding of the entity's cyber posture relating to external dependencies
  - Identification of improvement areas for managing third parties that support the organization



CISA
CYBER+INFRASTRUCTURE

TLP: GREEN

EDM Assessment Organization and Structure

- Structure and scoring similar to Cyber Resilience Review
- Also employs Maturity Indicator Level (MIL) scale across three lifecycle domains.

Relationship Formation *Assesses whether the acquirer evaluates and controls the risks of relying on external entities before entering into relationships with them.*
Relationship Management and Governance *Assesses whether the acquirer manages ongoing relationships to maintain the resilience of the critical service, and mitigate dependency risk.*
Service Protection and Sustainment *Assesses whether the acquirer accounts for its dependence on external entities as part of its operational activities around managing incidents, disruptions, and threats.*

Ransomware Readiness Assessment (RRA)

- Voluntary Self Assessment Module of the Cybersecurity Evaluation tool (CSET)

- Helps organizations evaluate their cybersecurity posture, with respect to ransomware, against recognized standards and best practice recommendations in a systematic, disciplined, and repeatable manner.

- Guides asset owners and operators through a systematic process to evaluate their operational technology (OT) and information technology (IT) network security practices against the ransomware threat.

- Provides analysis with graphs and tables that present the assessment results in both summary and detailed form.

Cyber Security Evaluation Tool (CSET)

- **Purpose:** Standalone “no-cost” software tool that runs on desktop/laptop. Contains 49 different best practices and industry standards to help organizations identify and prioritize cybersecurity concerns.
- **Facilitated:** Self-Administered, undertaken independently
- **Benefits:**
  - Immediately available for download upon request
  - Understanding of operational technology and information technology network security practices
  - Ability to drill down on specific areas and issues
  - Helps to integrate cybersecurity into current corporate risk management strategy

CISA
CYBER+INFRASTRUCTURE

TLP: GREEN

CSET Capabilities

What CSET CAN do:

- Provide a consistent means of evaluating a control system network as part of a comprehensive cybersecurity assessment
- Specify cybersecurity recommendations
- Report using standards-based information analysis
- Provide a baseline cybersecurity posture

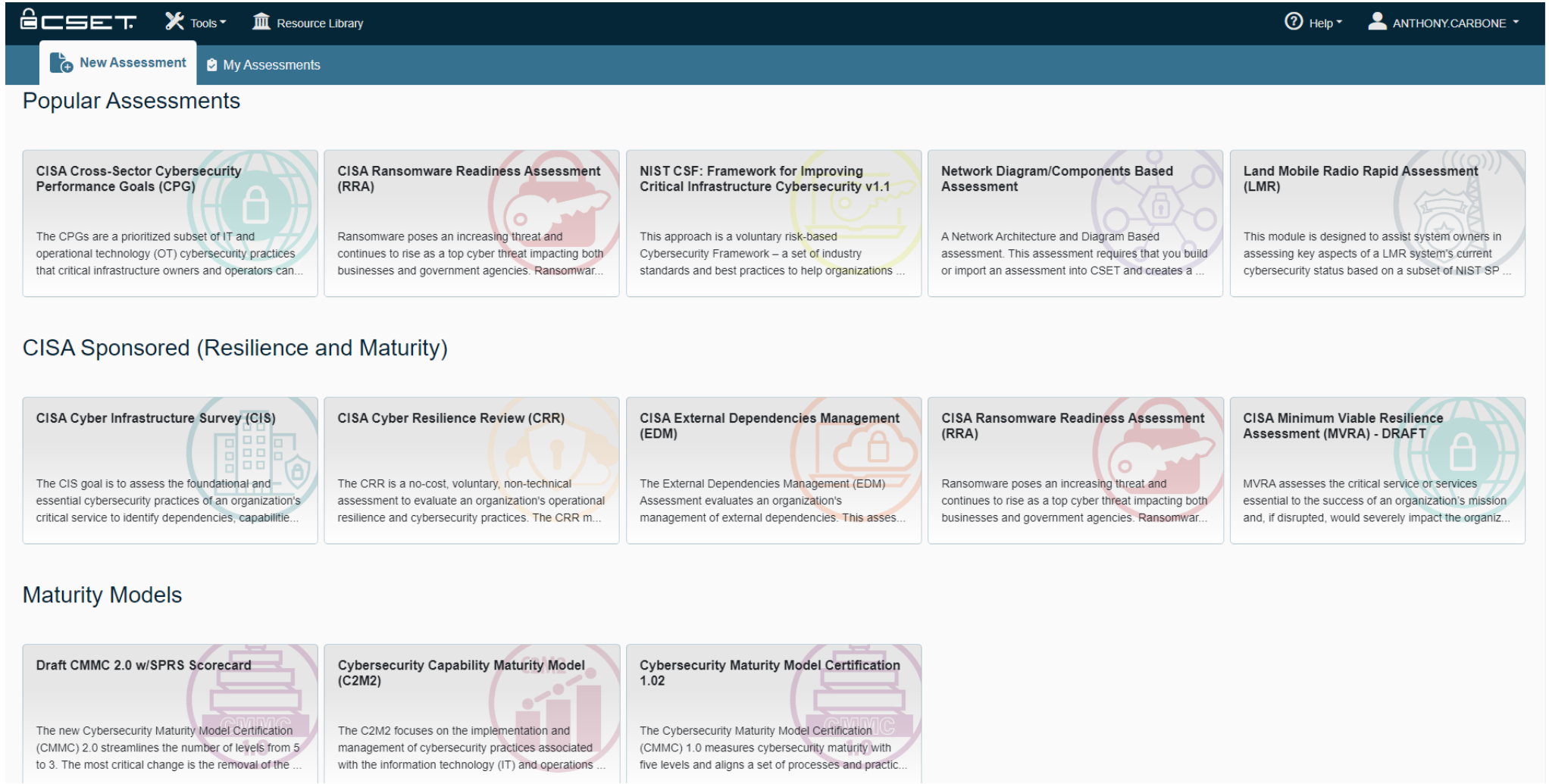
What CSET CAN NOT do:

- Validate accuracy of user inputs
- Ensure compliance with organizational or regulatory cybersecurity policies & procedures
- Ensure implementation of cybersecurity enhancements or mitigation techniques
- Identify all known cybersecurity vulnerabilities

CISA
CYBER+INFRASTRUCTURE

TLP: GREEN

CSET At A Glance



CISA
CYBER+INFRASTRUCTURE

TLP: GREEN

INFORMATION SHARING

Protected Critical Infrastructure Information Program

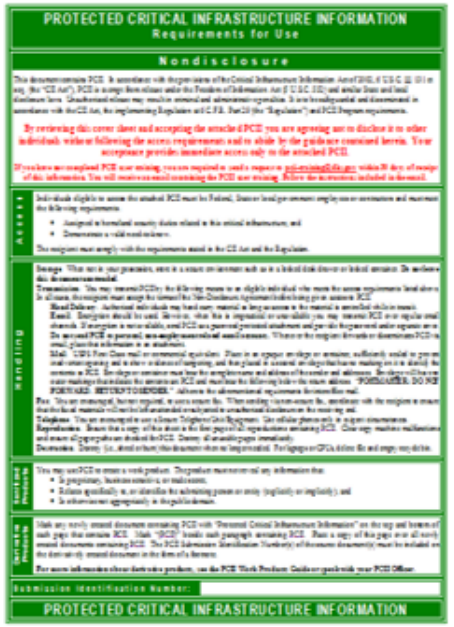
Purpose A **nationwide** program supporting DHS, other Federal Agencies, and SLTT governments to **encourage** critical infrastructure (CI) owners in private and SLTT sectors to ***voluntarily*** submit critical infrastructure information (CII) to the government.

Protections Protects Critical Infrastructure Stakeholders from the ***federal government***

- Disclosing information through the Freedom of Information Act (FOIA)
- Disclosing information through State & Local Government Disclosure Laws
- Using in Civil Actions
- Using in Regulatory Proceedings

Authorities

- Critical Infrastructure Information (CII) Act of 2002
- 6 Code of Federal Regulations part 29 (2022) (Tech Edits Completed)
- PCII Program Procedures Manual (2009) (Under Review)
- DHS Management Directive 262-08, PCII Program (2016)


PROTECTED CRITICAL INFRASTRUCTURE INFORMATION
Requirements for Use
Nondisclosure
PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

*The submission is protected immediately upon the federal government's receipt and throughout the validation process.

For more information on the electronic submission process, visit cisa.gov/electronic-submit-cii-pcii-protection

Additional Information Sharing Opportunities

- **ISACs and ISAOs:**
  - **Information Sharing and Analysis Centers** (ISACs) or **Organizations** (ISAOs) are communities of interest sharing cybersecurity risk, threat information, and incident management to members. For more information on ISACs, visit www.nationalisacs.org. For more on ISAOs visit www.isao.org/about.
- **Multi-State Information Sharing and Analysis Center:**
  - Focal point for cyber threat prevention, protection, response and recovery for state, local, tribal, and territorial governments.
  - Operates 24 x7 cyber security operations center, providing real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response. For more information, visit www.cisecurity.org/ms-isac or email info@msisac.org

Surface Transportation Information Sharing and Analysis Center — Over the Road Bus — Public Transportation — 24/7 Threat Warning & Incident Reporting

Elections Infrastructure ISAC

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

ONG-ISAC

National Defense ISAC

WATER ISAC

Real Estate ISAC Information Sharing and Analysis Center — Serving the Commercial Facilities Sector

H-ISAC HEALTH - ISAC

SPACE ISAC

DNG-ISAC

AUTO-ISAC Automotive Information Sharing and Analysis Center

AVIATION ISAC

Maritime Transportation System Information Sharing and Analysis Center

RETAIL & HOSPITALITY ISAC

REN-ISAC

CISA CYBER+INFRASTRUCTURE

MEISAC MEDIA + ENTERTAINMENT INFORMATION SHARING ANALYSIS CENTER

FS-ISAC

IT ISAC

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

TLP: GREEN

Incident Reporting

Why report cyber incidents?

- For situational awareness
- For decision making
- Requesting response assistance

When to report a cyber incident?

If there is a suspected or confirmed cyber attack or incident that:

- Affects core or critical business functions;
- Results in the loss of data, system confidentiality, integrity, and/ or availability; or control of systems;
- Indicates malicious software is present on critical systems

Who to report cyber incidents to?

- Leadership, public affairs, legal and other internal stakeholders
- Relevant vendors
- Law enforcement and other government agencies
- Cyber insurance providers
- Appropriate 3rd party incident response teams

CISA CYBER+INFRASTRUCTURE

TLP: GREEN

Asset Response:

CISA Central - Provides Real-Time Threat Analysis and Incident Reporting Capabilities

24x7 Contact:

- Dial: 1-888-282-0870
- Email: Central@cisa.dhs.gov
- Web: www.cisa.gov/report

Threat Response (NC):

NCDIT (State) or NCEM (Local, Academic, Private)

24x7 Contact:

- NCDIT: 800-722-3946 or DITThreatManagement@nc.gov
- NCEM: 800-858-0368 or NCEOC@ncdps.gov

Threat Response (SC):

South Carolina Law Enforcement Division Critical Infrastructure Cybersecurity (SLED CIC)

Contact:

- Dial: 803-896-8181
- Email: cyber@sled.sc.gov

CIRCIA

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

- Regulatory Requirement: Requires CISA to establish a new regulatory program requiring reporting of certain cybersecurity related information:
  - **Covered entities** must report to CISA **covered cyber incidents** **within 72 hours** after the entity reasonably believes that a covered cyber incident occurred
  - **Covered entities** must report to CISA any ransomware payments **within 24 hours of making the payment**
- Requires CISA to coordinate with Federal SRMA partners on various cyber incident reporting and ransomware related activities
- CIRCIA Reports may receive information protections listed under 6 U.SC. 681e.
- Rulemaking comment period ended on 3-July-2024.
- CIRCIA reporting requirements is not required until after the final rule issued and effective *(~Q4, 2025)*

CISA CYBER+INFRASTRUCTURE

ADDITIONAL CYBERSECURITY RESOURCES

Cybersecurity & Resilience Resources

https://www.cisa.gov/shields-up

CISA
CYBER+INFRASTRUCTURE

Cyber Exercises and Planning

CISA's National Cyber Exercise and Planning Program develops, conducts, and evaluates cyber exercises and planning activities for state, local, tribal and territorial governments and public and private sector critical infrastructure organizations.

- Cyber Storm Exercise – DHS's flagship national-level biennial exercise
- Exercise Planning and Execution
- Cyber Exercise Consulting and Subject Expertise Support
- Cyber Planning Support
- Off-the-Shelf Resources

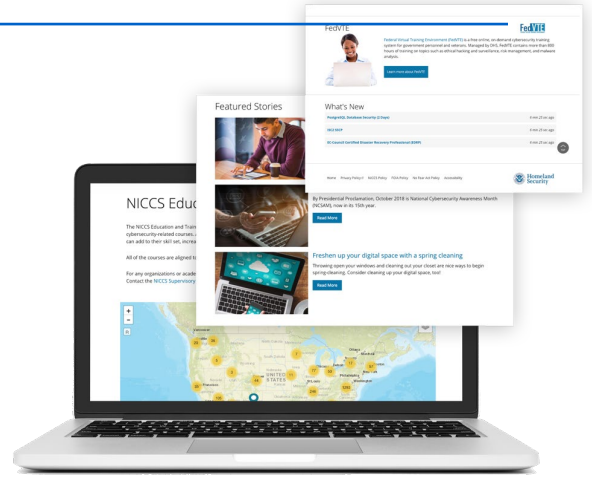
CISA
CYBER+INFRASTRUCTURE

TLP: GREEN

Cybersecurity Training Resources

CISA is committed to providing the nation with access to cybersecurity training and workforce development efforts to develop am ore resilient and capable cyber nation.

- **The NICCS website** is a searchable training catalog with over 6000 cyber-related courses offered by nationwide cybersecurity educators
  - Interactive National Cybersecurity Workforce Framework
- FedVTE
- Scholarships for Service, Centers for Academic Excellence, and Cyber Competitions
- Tools and Resources for Cyber Managers
- Incident Response Training Through Identify, Mitigate, Recover (IMR) Series
- Industrial Control System Cybersecurity Training



CISA CYBER+INFRASTRUCTURE

For More Information, Visit: https://www.cisa.gov/cybersecurity-training-exercises

TLP: GREEN

Our Nation's Cyber Workforce Foundation

The **National Cybersecurity Workforce Framework** is a collection of definitions that describe types of cybersecurity work and skills requires to perform it.

- ✓ When used nationally, the definitions help establish universally applicable cybersecurity skills, training/development, and curricula
- ✓ 7 Categories, 30+ Specialty Areas
- ✓ Baselines knowledge, skills, and abilities & tasks

Operate & Maintain | **Securely Provision** | **Analyze** | **Collect & Operate** | **Oversight & Development** | **Protect & Defend** | **Investigate**

For more information, visit https://www.cisa.gov/nice-cybersecurity-workforce-framework

CISA
CYBER+INFRASTRUCTURE

No-Cost Cybersecurity Tools (Hyperlinked)

Assess Vulnerabilities:

- Downloading and Installing CSET | CISA
- Known Exploited Vulnerabilities Catalog | CISA

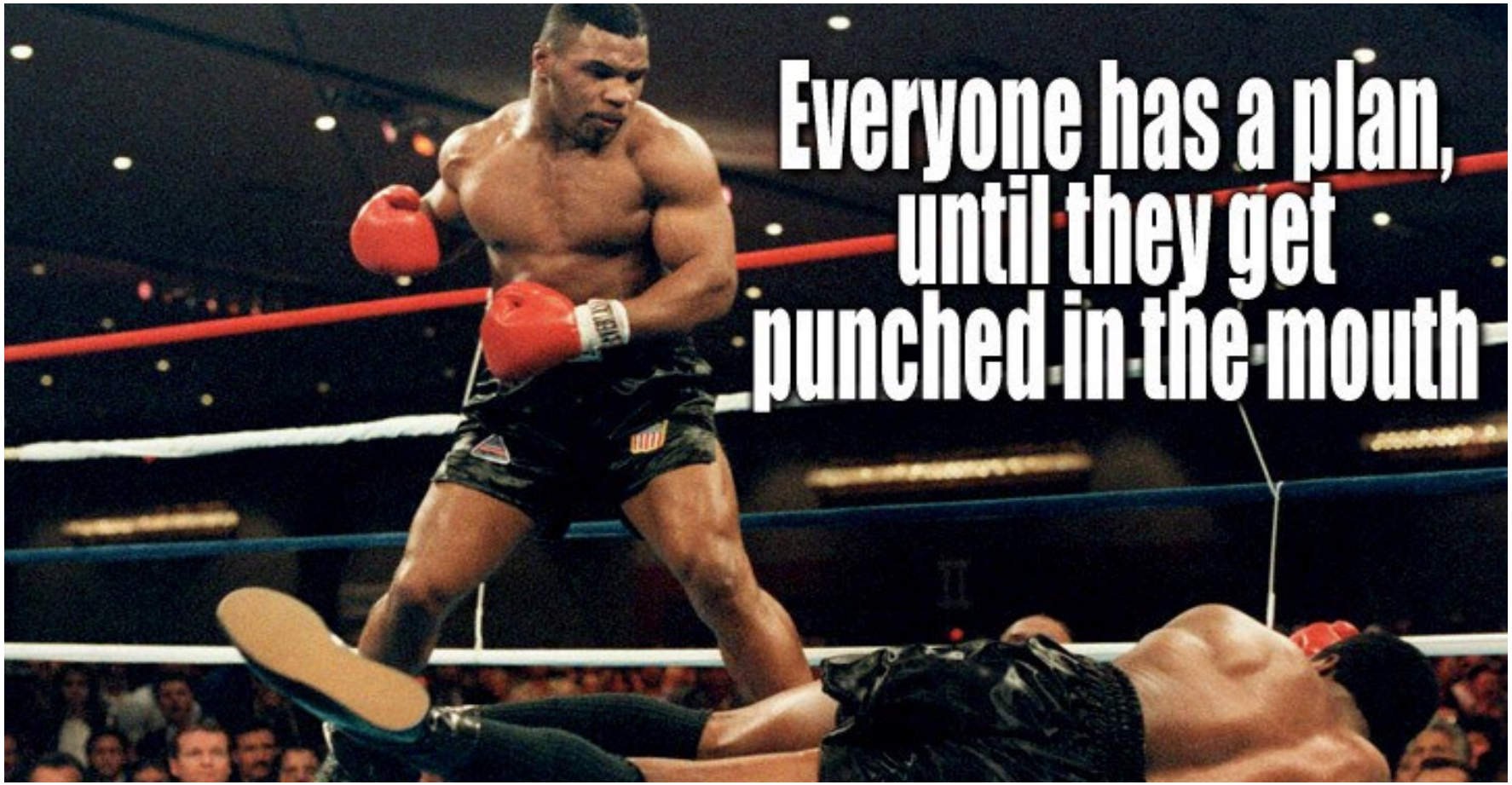
Hardening:

- CIS Benchmarks (cisecurity.org)
- GitHub - decalage2/awesome-security-hardening: A collection of awesome security hardening guides, tools and other resources
- Secure Cloud Business Applications (SCuBA) Project | CISA
  - GitHub - cisagov/ScubaGear: Automation to assess the state of your M365 tenant against CISA's baselines
  - https://www.cisa.gov/sites/default/files/publications/SCuBA_TRA_RFC_EG_508c.pdf

Cyber Defense:

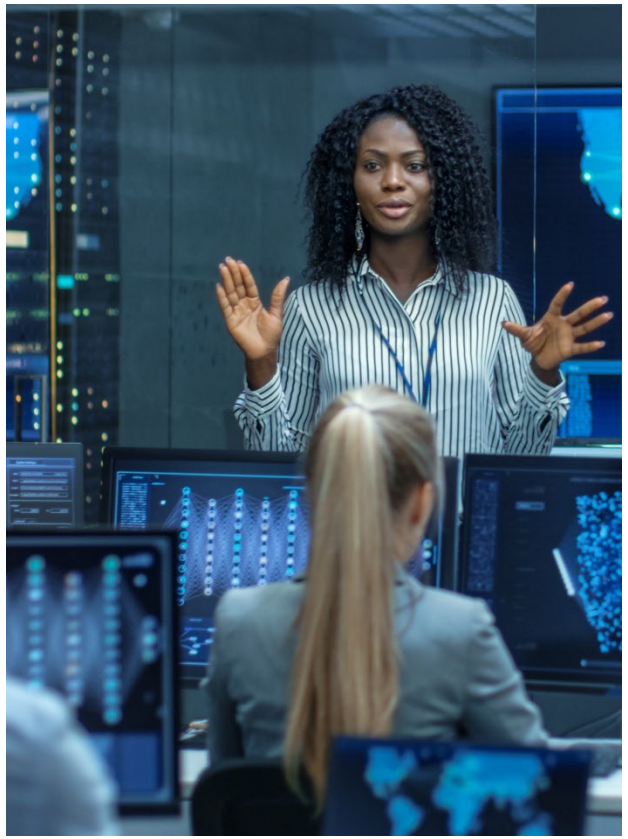
- Helping Cyber Defenders "Decide" to Use MITRE ATT&CK | CISA
- Untitled Goose Tool Fact Sheet | CISA (Azure)
- CISA Releases RedEye: Red Team Campaign Visualization and Reporting Tool | CISA
- CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks | CISA

Bottom Line



CISA
CYBER+INFRASTRUCTURE

Contact



General Inquiries

CISARegion4@hq.dhs.gov

CISA Contact Information

Rob Main **CSC - Raleigh NC** **CISA Region 4**	**Rob.Main@cisa.dhs.gov**

CISA Resource Hub

https://www.cisa.gov/cyber-resource-hub

Questions / Next Step

General Inquiries

cisa.iod.region.r04_ops@cisa.dhs.gov

Columbia

PSA Keith Jones	CSC CL Clay
Email: keith.m.jones@hq.dhs.gov Cell: 803.218.8550	Email: cl.clay@cisa.dhs.gov Cell: 771.217.7652

Charleston / Mt. Pleasant

PSA Amanda Knight	CSA Anthony E. Carbone
Email: amanda.knight@cisa.dhs.gov Cell: 771.217.1409	Email: anthony.carbone@cisa.dhs.gov Cell: 771.215.7508

CISA CYBER+INFRASTRUCTURE

CISA

CYBER+INFRASTRUCTURE

TLP: GREEN