CISA Capabilities Brief

FACT Risk Management Conference

PSA Kirby Wedekind
October 30, 2019

Agenda

- CISA Vision, Mission, and Strategy
- Protective Security & Cybersecurity Advisors
- Cybersecurity Assessments
  - Cybersecurity Advisors
  - National Cybersecurity Assessments and Technical Services (NCATS)Cyber Incident Response
- Information Sharing

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

A Nation with secure and resilient critical infrastructure that ensures our security, economic prosperity, and way of life.

MISSION

Strengthen the Nation's cyber and physical infrastructure by managing and reducing systemic and catastrophic risk in partnership with the private sector, collaboration with the public sector, and protection of federal government networks.

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Who We Are

CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

FEDERAL NETWORK PROTECTION

PROACTIVE CYBER PROTECTION

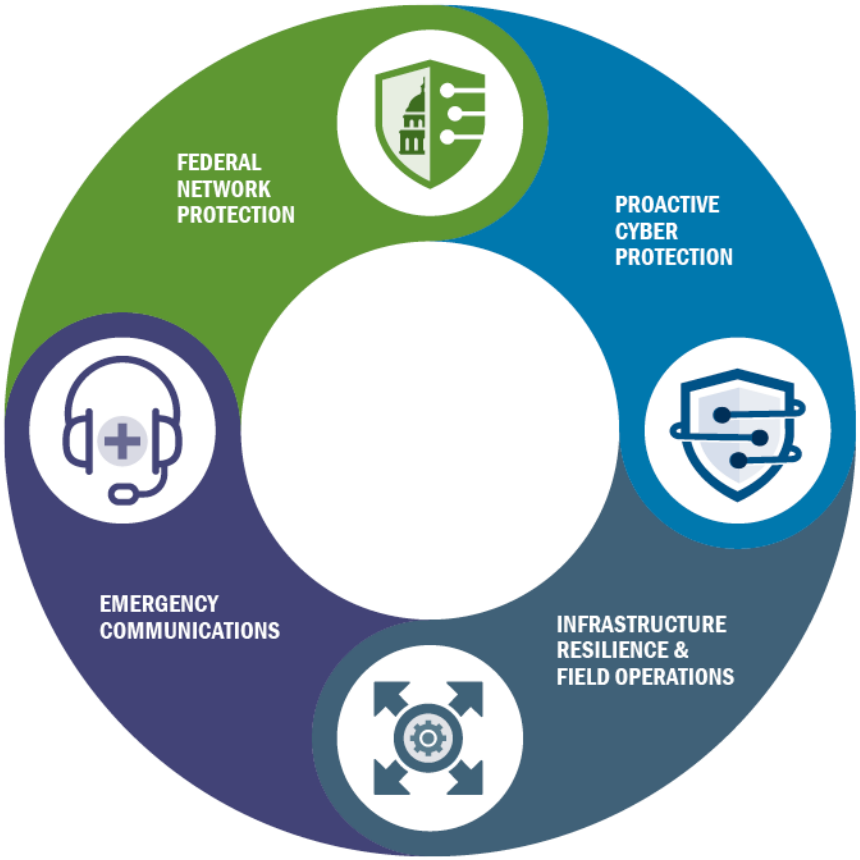
INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS

EMERGENCY COMMUNICATIONS

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



Protective Security Advisors

- Engage proactively with federal, state, local, tribal, and territorial government partners and members of the private sector to protect critical infrastructure through five mission areas:
  - Security and resilience surveys and assessments
  - Outreach that provides access to security and resilience resources, training, and information
  - Liaise between government officials and the private sector during and after an incident or special event
  - Facilitating improvised explosive device awareness, risk mitigation training, and CISA's cybersecurity resources

Cybersecurity Advisors

- Offer assistance to help prepare and protect private sector entities and SLTT governments from cybersecurity threats
- Promote cybersecurity preparedness, risk mitigation, and incident response capabilities, working to engage stakeholders through partnership and direct assistance activities
  - Cyber Preparedness
  - Strategic Messaging
  - Working Group Support
  - Partnership Development
  - Cyber Assessments
  - Incident Coordination and Support

Protected Critical Infrastructure Information

- Established under the Critical Infrastructure Information Act of 2002
- Protects voluntarily submitted critical infrastructure information from:
  - Freedom of Information Act
  - State and local sunshine laws
  - Civil litigation proceedings
  - Regulatory usage
- Provides legal protections to proprietary information

Cyber Resilience Review

- Evaluates the maturity of an organization's capabilities and capacities in performing, planning, managing, measuring, and defining cybersecurity capabilities across the following 10 domains:
  - Asset Management
  - Controls Management
  - Configuration and Change Management
  - Vulnerability Management
  - Incident Management
  - Service Continuity Management
  - Risk Management
  - External Dependency Management
  - Training and Awareness
  - Situational Awareness

Cyber Resilience Review

- Value provided:
  - Improved enterprise-wide awareness of the need for effective cybersecurity management
  - A review of capabilities essential to the continuity of critical services during operational challenges and crisis
  - Integrated peer performance comparisons for each of the 10 domains covered in the assessment
  - A comprehensive final report that includes options for improvement

Cyber Infrastructure Survey

- Evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and overall resilience of the cybersecurity ecosystem
- Provides service-based as opposed to programmatic view
- Critical services are assessed against more than 80 cybersecurity controls grouped into the following 5 top-level domains:
  - Cybersecurity Management
  - Cybersecurity Forces
  - Cybersecurity Controls
  - Cybersecurity Incident Response
  - Cybersecurity Dependencies

Cyber Infrastructure Survey

- Value provided:
  - Effective assessment of critical service cybersecurity controls
  - Interactive dashboard to support cybersecurity planning and resource allocation
  - Peer performance data visually depicted on the dashboard
  - User-friendly dashboard to review the results and findings of the survey
- Contact: **Region4CSA@cisa.dhs.gov**

External Dependencies Management

- Interview-based assessment that evaluates an organization's management of external dependencies
  - Focuses on the relationship between an organization's high-value services and assets (i.e., people, technology, facilities, & information)
  - Evaluates management of risk derived from Information and Communications Technology (ICT) Supply Chain
    - Relationship formation
    - Relationship management and governance
    - Service protection and sustainment

External Dependencies Management

- Value provided:
  - Opportunity for internal discussion of vendor-related issues and the organization's reliance upon external entities in order to provide services
  - Improvement options for consideration derived from recognized standards and best practices
  - A comprehensive report on the organization's third-party risk management practices and capabilities that includes peer performance comparisons
- Contact: **Region4CSA@cisa.dhs.gov**

National Cybersecurity Assessments and Technical Services (NCATS)

- Provides objective, third-party testing and assessment services of operational cybersecurity posture
- Identifies security control strengths and weaknesses
- Delivers reports that can inform prioritization of vulnerabilities and allocation of resources
  - Port scanning / Penetration Testing
  - Phishing Campaign Assessment
  - Network Mapping

Cyber Hygiene: Vulnerability Scanning

- What it does:
  - Identifies all active Internet accessible assets (networks, systems and hosts) to be scanned for vulnerabilities
  - Performs regular network and vulnerability scans through voluntary target discovery, vulnerability scanning, and checks of web and email best practices
- Value Provided:
  - Once initiated, automated and requires little direct interaction
  - Helps secure internet-facing systems from weak configuration and known vulnerabilities

Contact: **Region4CSA@cisa.dhs.gov**

Phishing Campaign Assessment

- What it does:
  - Measures susceptibility to social engineering attacks, specifically email phishing attacks over a 6 week period
  - Focuses on user behavior
- Value Provided:
  - Phishing campaign statistics, findings, and associated remediation steps
  - Results can be used to provide guidance for anti-phishing training and awareness
- Contact: **Region4CSA@cisa.dhs.gov**

CISA
CYBER+INFRASTRUCTURE

Risk and Vulnerability Assessment

- What it does:
  - Full penetration test
  - Technical phishing assessment
  - Web application assessment
  - Wireless access point detection and penetration testing
  - Operating System Security Assessment
  - Database assessment
  - War Dialing

Risk and Vulnerability Assessment

- Value Provided:
  - Identifies vulnerabilities across a range of cybersecurity areas
  - Provides recommended mitigation steps associated with best practices (e.g., OWASP Top Ten, NIST CSF, USG or CIS recommended baselines, etc.)
  - Provides a neutral, third-party perspective
  - Tailorable rules of engagement
- Contact: **Region4CSA@cisa.dhs.gov**

Remote Penetration Testing

- Utilizes a dedicated remote team to assess and identify and mitigate vulnerabilities to exploitable pathways
- While similar to a Risk and Vulnerability Assessment, Remote Penetration Testing focuses entirely on externally accessible systems
- Methodologies may include:
  - Scenario-based external network penetration testing
  - External web application testing
  - Phishing Campaign Assessment

Remote Penetration Testing

- Value provided:
  - Receive a final report that includes business executive recommendations, specific findings and potential mitigations, as well as technical attack path details
  - An optional debrief presentation summarizing preliminary findings and observations is also available
- Contact: **Region4CSA@cisa.dhs.gov**

Validated Architecture Design Review

- What it does:
  - Table-top assessment based on standards, guidelines, and best practices that can encompass both Information Technology (IT) and Operational Technology (OT) systems and networks
  - Evaluates systems, networks, and security services to determine if designed, built, and operated in a reliable and resilient manner
    - Review IT and OT system and program practices against best practices for system components and architectures, and operational policies and procedures
    - Perform Network Architecture Review
    - Perform Network Header Data Analysis
    - Perform System Log Review
    - Review system configuration files

Validated Architecture Design Review

- Value Provided:
  - Report detailing observed strengths and discoveries identified
  - Each discovery identified is linked to the Cybersecurity Framework, NIST 800-82, or NIST 800-83, an associated consequence, and a recommendation for mitigation
- Contact: **Region4CSA@cisa.dhs.gov**

Cyber Incident Reporting

- Cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems.
- Cyber incidents resulting in significant damage are of particular concern to the Federal Government.
  - Significant loss of data, system availability, or control of systems
  - Impact a large number of victims
  - Indicate unauthorized access to, or malicious software present on, critical information technology systems
  - Affect critical infrastructure or core government functions
  - Impact national security, economic security, or public health and safety

Cyber Incident Response

- National Cybersecurity and Communications Integration Center (NCCIC) serves as a national center for reporting and mitigating communications & cybersecurity incidents
- Provides alerts and warnings on cyber and communications incidents
- To report a cyber incident:
  - Email: **NCCICCustomerService@us-cert.gov**
  - Call: 703-235-8832
  - Call: 888-282-0870

Cyber Incident Response

- Hunt and Incident Response Team (HIRT) provides incident response, management and coordination activities for cyber incidents
  - Remote, On-Site, and Advisory Services
  - Private industry / Critical infrastructure sectors
  - Federal, State, Local, Tribal, and Territorial government organizations
- Upon completion of analysis, the HIRT will deliver an Engagement Report (ER) to the customer within 30-60 days that provides the background, scope, findings, security best practices, and conclusions relevant to the hunt

Cyber Incident Response

- E-mail to: **submit@malware.us-cert.gov**
  - Password protect the submission using the password “infected”
  - Do not use any custom passwords or encryption methods other than zip or 7z
  - The samples are received/processed by an automated system that only knows these archive formats and this password.
  - Please do not include any other addressee on your submission message(s) to prevent inadvertent infection of recipients.

Cyber Incident Response

- Web submission to: **https://malware.us-cert.gov**
  - Submissions to this location can be encrypted or unencrypted
- Web submission to: **ftp.malware.us-cert.gov/malware**
  - Anonymous credentials to access
  - Used for submitting files too large for email (e.g., forensic data, images, logs)
  - 1 TB limit
  - Submitters should include a readme file with NCCIC ticket number and POC information

Cyber Incident Response

- FBI: Internet Crime Complaint Center (IC3)
  - Facilitates reporting suspected criminal activity via internet
  - Examples of online fraud:
    - Intellectual Property Rights (IPR) matters
    - Computer Intrusions (hacking)
    - Economic Espionage (Theft of Trade Secrets)
    - Online Extortion
    - International Money Laundering
    - Identity Theft
- Visit: **https://www.ic3.gov/default.aspx**

Information Sharing

- National Cyber Awareness System
  - High-impact types of security activity
  - Timely information about current security issues, vulnerabilities, and exploits
  - Weekly summaries of new vulnerabilities (+patch information is provided when available)
  - Advice about common security issues for the general public
  - Analysis Reports provide in-depth analysis on a new or evolving cyber threat
- Visit: **https://www.us-cert.gov/ncas**

Information Sharing

- National Cyber Awareness System
  - Industrial Control Systems Alerts provide timely notification concerning threats or activity with the potential to impact critical infrastructure computing networks
  - •Industrial Control Systems Advisories provide timely information about current industrial control systems (ICS) security issues, vulnerabilities, and exploits
- Visit: **https://www.us-cert.gov/ncas**

Information Sharing

- Florida Fusion Center: FloridaFusionCenter@fdle.state.fl.us
- Northwest Florida Fusion Center: nwfloridafusion@fdle.state.fl.us
- North Florida Fusion eXchange: nffx@flcjn.net
- Northeast Florida Fusion Center: contact@northeastfloridafusion.org
- Tampa Bay Regional Intelligence Center: TBRIC@fdle.state.fl.us
- Central Florida Intelligence eXchange: CFIX@ocfl.net
- Southeast Florida Fusion Center: seffc@mdpd.com & fusion@pbso.org
- Southwest Florida Fusion Center: RSIX@fdle.state.fl.us

Information Sharing

- Homeland Security Information Network (HSIN)
  - Based on Communities of Interests that focus on either functional and geographic areas
  - Cyber Intelligence Network (CIN)
- How to connect with cyber information:
  1. Signup for NCAS Alerts
  2. Connect with the fusion center in your area
  3. Register for an HSIN account
  4. Join Communities of Interest
  5. Proactively engage and share information with partners

Additional Topics

- Physical Security Vulnerability Assessments
- Special Events & Incident Response
- Elections Security
- Places of Worship & Faith-Based Organizations
- K-12 Schools & Institutes of Higher Education
- Suspicious Activity, Behavior, & Insider Threat
- Unmanned Aircraft Systems

CISA
CYBER+INFRASTRUCTURE

For more information:

cisa.gov

Questions?

Email: Kirby.Wedekind@hq.dhs.gov
Phone: 202 868 1361

CISA

CYBER+INFRASTRUCTURE