
CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

CISA partners with industry and government to understand and manage risk to our Nation's critical 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

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future

PARTNERSHIP DEVELOPMENT

INFORMATION AND DATA SHARING

CAPACITY BUILDING

INCIDENT MANAGEMENT & RESPONSE

RISK ASSESSMENT AND ANALYSIS

NETWORK DEFENSE

EMERGENCY COMMUNICATIONS

CISA Operational Priorities

CYBER SUPPLY CHAIN AND 5G

CISA is focused on supply chain risk management in the context of national security. CISA is looking to reduce the risks of foreign adversary supply chain compromise in 5G and other technologies.

ELECTION SECURITY

CISA assists state and local governments and the private sector organizations that support them with efforts to enhance the security and resilience of election infrastructure. CISA's objective is to reduce the likelihood of compromises to election infrastructure confidentiality, integrity, and availability, essential to the conduct of free and fair democratic elections.

SOFT TARGET SECURITY

As the DHS lead for the soft targets and crowded places security effort, CISA supports partners to identify, develop, and implement innovative and scalable measures to mitigate risks to these venues; many of which serve an integral role in the country's economy.

FEDERAL CYBERSECURITY

CISA provides technology capabilities, services, and information necessary for agencies across the Federal civilian executive branch to manage sophisticated cybersecurity risks. CISA's authorities enable deployment of robust capabilities to protect Federal civilian unclassified systems, recognizing that continuous improvement is required to combat evolving threats. CISA also works to help State, Local, Tribal and Territorial governments improve cybersecurity and defend against cybersecurity risks.

INDUSTRIAL CONTROL SYSTEMS

CISA leads the Federal Government's unified effort to work with the Industrial control systems (ICS) community to reduce risk to our critical infrastructure by strengthening control systems' security and resilience.

Enhancing Pipeline Cybersecurity (SDP-2021-01)

Pipeline Security Directive: Requires three critical actions!

1. Owner/Operators must report cybersecurity incidents
2. Designate a Cybersecurity Coordinator to be available to TSA and CISA
3. Owner/Operators must review current activities against TSA recommendations:
   a) Assess cyber risk
   b) Identify gaps
   c) Develop remediation measures
   d) Report results to TSA and CISA

Geoff Jenista, CISSP
October 28, 2021

Cybersecurity Trends

Five most prevalent cybersecurity threats:

- E-mail phishing attacks (92% of all attacks)
- Ransomware attacks
- Loss or theft of equipment or data
- Insider, accidental or intentional data loss
- Attacks against connected devices
  - Printers, Cameras, Wireless Devices (Mouse)
  - Business Wireless Access

Cyber Threats of Today

Ransomware

- WannaCry
- REvil/Sodinokibi (targeting MSPs)
- Ryuk (targeting medical, education, SLTT)
- Conti, Robinhood, Maze, Fobos, CovidLock, CryptoLocker, Pysa, VoidCrypt…

Malware

- Remote Access Trojans or RATs: **Trickbot**, Emotet, LokiBot, IcedID, BazarLoader
- Wiperware NotPetya
- ICS/OT specific: Triton/hatman malware targets Safety Instrumented Systems (SIS)

Advanced Persistant Threats (APTs)

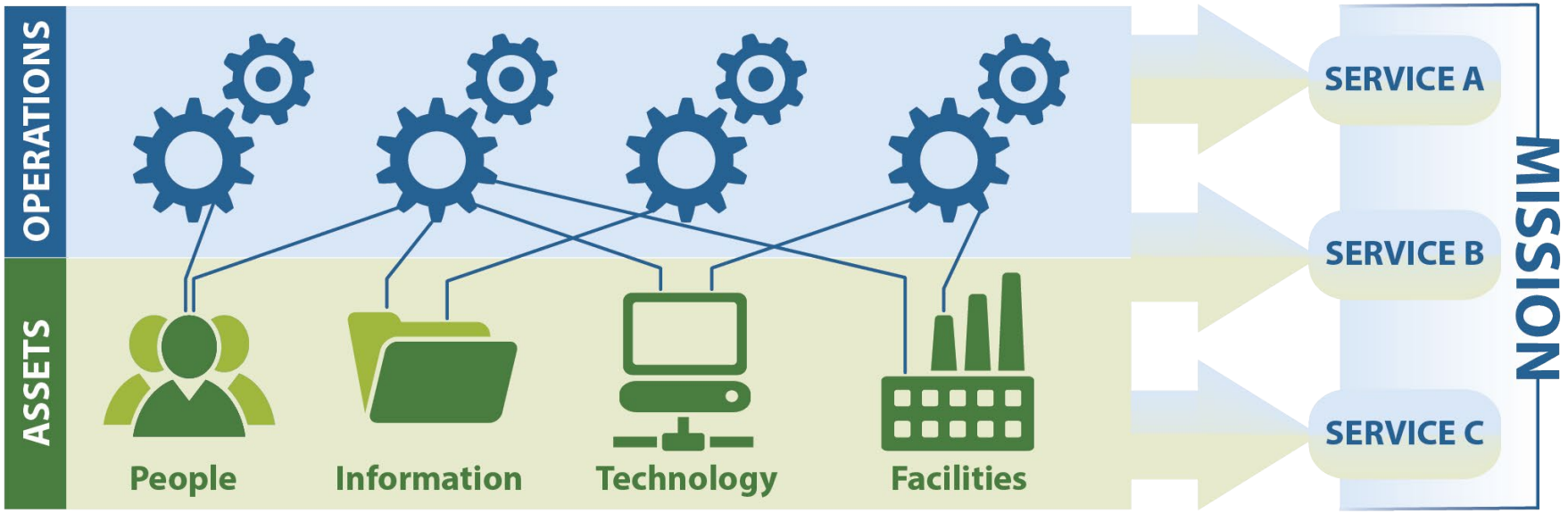
- Energetic Bear/Berserk Bear (targets U.S. state, local, territorial, and tribal (SLTT) government networks, as well as aviation networks)

Threats to External Dependencies

- 3rd party vendors, service providers, infrastructure providers
- Supply chain Compromise

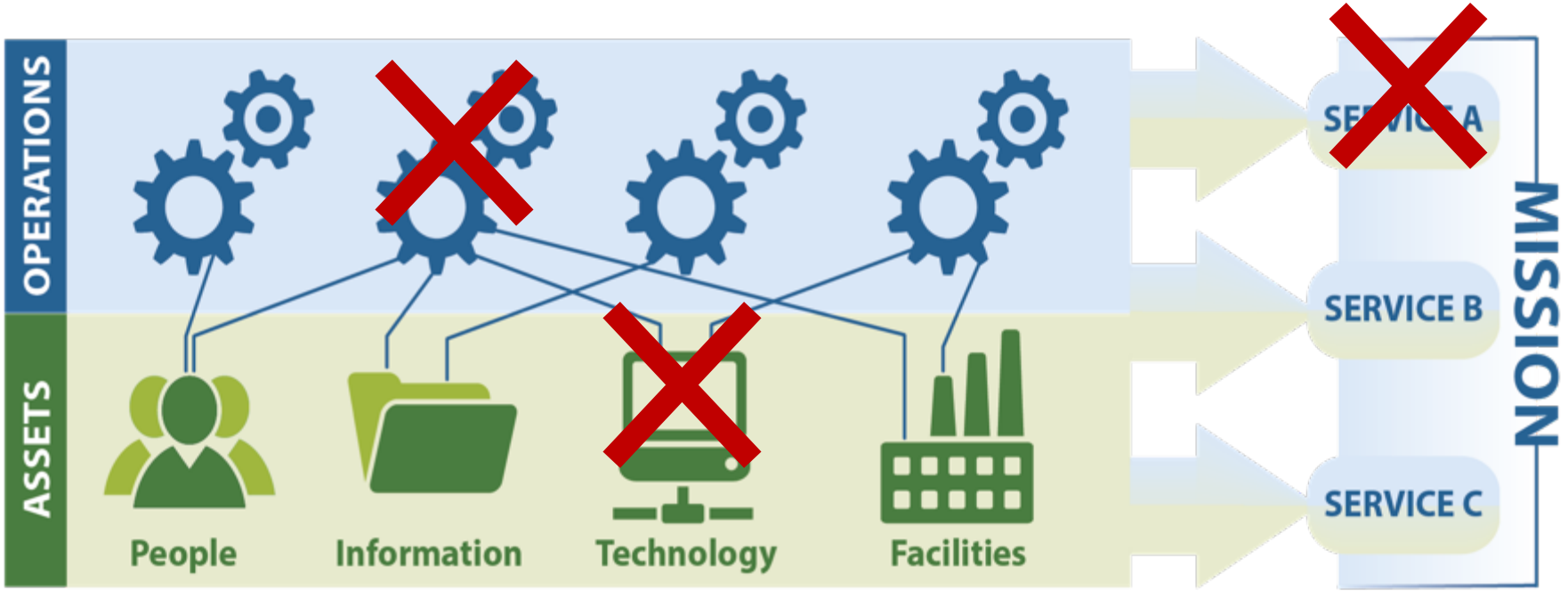
Defining the Critical Service

An organization uses its **assets (people, information, technology, and facilities)** to perform **productive activities** to provide operational **services** and accomplish the organization's **mission.**



Critical Service Focus

Organizations use **assets (people, information, technology, and facilities)** to provide operational **services** and accomplish **missions.**



Geoff Jenista, CISSP
October 28, 2021

How do we think about risk?

Operational Risk = $\frac{\text{Threats x Vulnerabilities x Consequence}}{\text{Controls}}$

THREAT (T)

Likelihood that a particular asset, system, or network will suffer an attack or an incident

VULNERABILITY (V)

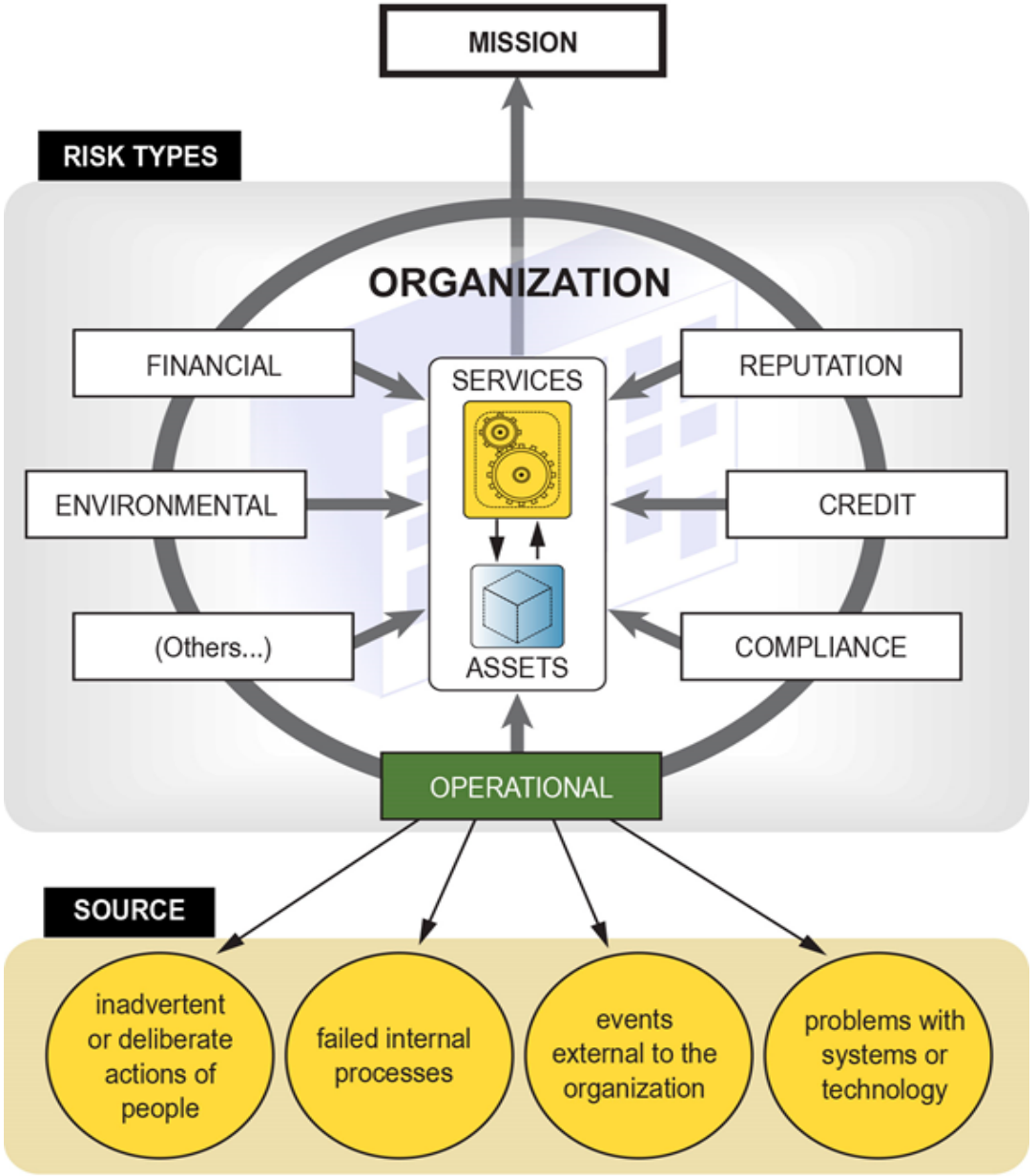
Likelihood that a characteristic of, or flaw in, an asset, system, or network renders it susceptible to hazards

CONSEQUENCE (C)

Negative effects on public health and safety, the economy, public confidence in institutions, and function of government if asset, system, or network is damaged, destroyed, or disrupted

Increasing the Focus on Operational/Cyber Risk

TLP:WHITE



Geoff Jenista, CISSP
October 28, 2021

Risk-Based Performance Standards

1) Restrict Area Perimeter

2) Secure Site Assets

3) Screen and Control Access

4) Deter, Detect, Delay

5) Shipping, Receipt, and Storage

6) Theft and Diversion

7) Sabotage

8) Cyber

9) Response

10) Monitoring

11) Training

12) Personnel Surety

13) Elevated Threats

14) Specific Threats, Vulnerabilities, or Risks

15) Reporting Significant Security Incidents

16) Significant Security Incidents and Suspicious Activities

17) Officials and Organization

18) Records

- Compliance with the RBPS will be tailored to fit each facility's circumstances, including tier level, security issues, and physical and operating environments
- Rather than prescribe specific facility security measures, DHS developed 18 Risk-Based Performance Standards (RBPS)

Risk-Based Performance Standards

- Risk-Based Performance Standards (RBPS) are the foundation of a facility's Site Security Plan and drive the security standards at all tiered facilities.
- RBPS provide facilities with flexibility and allow for the use of existing or planned measures, ideas, and expertise where appropriate.
- A covered high-risk facility has to satisfy the applicable RBPS by implementing security measures appropriate to the facility's risk tier.
- Security measures appropriate to satisfy the RBPS will vary from one facility to another based upon level of risk and unique facility circumstances.

Cybersecurity

- Computerized systems are replacing methods of business across numerous industries. As these methods change, so do the vulnerabilities that organizations face. Cyber intrusions to control systems and critical information are more common than ever which is why protecting against these cyber attacks is an essential component in managing overall risk for a facility.
- The goal of cybersecurity is to reduce the risk of attackers conducting malicious attacks on critical systems, which could result in theft, diversion, release, or sabotage.

RBPS 8 and Cyber Systems

RBPS 8 – Cyber addresses the deterrence of cyber sabotage, including preventing unauthorized on-site or remote access to critical process controls, critical business systems, and other sensitive computerized systems.

Examples of critical cyber systems include:

Physical Security Systems

- An access control or security system that is connected to other systems
  - Does the facility employ an intrusion detection system or cameras?

Inventory Management and Office Systems

- A business system that manages the ordering / shipping of a dangerous chemical
  - Does the facility utilize software to manage ordering, shipping, or inventory?

Automated Processing Systems

- A control system that monitors or controls physical processes
  - Does the facility employ control systems (ICS, DCS, SCADA)?

Business and Personnel Management (HR) Systems:

- E-mail or fax systems used to transmit sensitive information
- A non-critical control system on the same network as a critical control system
- Proprietary information, personal identifiable information (PII)

Cybersecurity Measures

The facility should implement measures for all of the identified systems:

Security Policy
- Policies on operational constraints, sensitivity issues, and processing issues

Access Control
- System boundaries, external connections, password management, etc.

Personnel Surety
- Unique accounts, separation of duties, access control lists, etc.

Awareness and Training
- Roles and responsibilities, password procedures, reporting incidents, etc.

Cybersecurity Controls, Monitoring, Response and Reporting
- Defense against viruses and monitoring facility networks, response methods to identify, contain, and resolve cyber intrusions, reporting incidents to US-CERT

Disaster Recovery and Business Continuity
- Cybersecurity considerations during contingency operations and **recovery back-ups**!

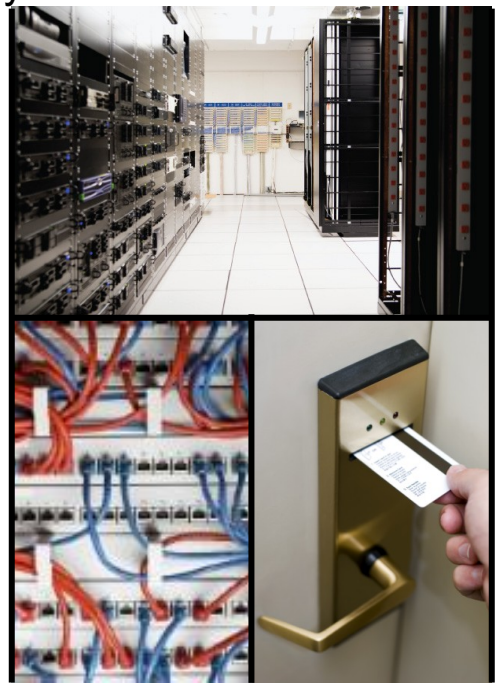
System Development and Acquisition
- Implementing cybersecurity throughout the system development life cycle

Configuration Management
- Maintaining inventory of cyber assets and system manuals

Audits
- Keeping records of audit reports to better understand and mitigate cyber threats

Cybersecurity Considerations

- **Potential Off-Site Aspect of Cybersecurity**
  - Multiple facility corporations can consider IT equipment, IT data, and IT staff to be located off-site or separate locations (e.g., selected sites, headquarters, third party)
- **Interconnectivity of Critical and Seemingly Non-Critical Systems**
  - Seemingly non-critical systems pose a potential risk of access to systems that manage critical processes when they are interconnected
- **Impact of Risk Drivers**
  - Securing facility systems considered cybersecurity risk drivers (e.g., process control systems for release facilities or shipment and customer database for theft facilities)
- **Physical Security for Cyber Assets**
  - Protecting cyber assets through restricting physical areas and role-based security
- **Layered Security**
  - Implementing multiple physical and cyber countermeasures for layers of security



DHS Cyber Security Offerings – CISA Central

Cyber Hygiene Scanning (CyHy):

- Broadly assess Internet-accessible systems for known vulnerabilities and configuration errors on a persistent basis.

Web Application Scanning (WAS):

- Broadly assesses the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Recommend ways to enhance security in accordance with industry and government best practices and standards.

Phishing Campaign Assessment (PCA):

- Measures susceptibility to email attack
- Delivers simulated phishing emails
- Quantifies click-rate metrics over a 6-week period

Remote Penetration Testing (RPT):

- Remote Penetration Test (RPT) utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways.

Cyber Security Advisor (CSA) Offerings

Cyber Resiliency Review (CRR):

- The Cyber Resilience Review (CRR) is a no-cost, voluntary, interview-based assessment to evaluate an organization's operational resilience and cybersecurity practices. (Strategic Report)

External Dependencies Management Assessment (EDM):

- The External Dependencies Management (EDM) assessment is a no-cost, voluntary, interview-based assessment to evaluate an organization's management of their dependencies. (Tactical Report)

Cyber Infrastructure Survey (CIS):

- The Cyber Infrastructure Survey (CIS) is a no-cost, voluntary survey that evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and overall resilience. (Operational Report)

Cyber Security Evaluation Tool (CSET):

- The CSET provides a systematic, disciplined, and repeatable method for assessing infrastructure; compare multiple assessments to establish a baseline and determine trends; controls priority list.

Protective Security Advisor (PSA) Offerings

All-Hazards Security Assessments

- Security Walkthrough Assessment
- Security Assessment at First Entry (SAFE)
- Infrastructure Survey Tool (IST) Assessment
- Multi-Asset and Systems Assessment

Training:

- Active Shooter - Employees
- Active Shooter Workshop – Leadership, Security & Emergency Managers
- Classroom courses:
  - Bombing Prevention/C-IED, Emergency Preparedness & Business Continuity

Outreach, Support & Resources:

- Critical Infrastructure Outreach & Speaking Engagements
- Incidents Response
- Special Event Security Planning
- Drills & Exercises
- Products: Protective Measures, Intelligence, GIS, Plume Modeling, Infrastructure Visualization Platform (IVP)

Cyber Security Framework

Functions	Categories
IDENTIFY (ID)	Asset Mangement (AM)
	Business Environment (BE)
	Governenace (GV)
	Risk Assessment (RA)
	Risk Management Stategy (RM)
PROTECT (PR)	Access Control (AC)
	Awareness and Training (AT)
	Data Security (DS)
	Information Protection Processess and Procedures (IP)
	Maintenance (MA)
	Protective Technology (PT)
DETECT (DE)	Anomolies and Events (AE)
	Security Continuos Monitoring (CM)
	Detection Processes (DP)
RESPOND (RS)	Incident Response Planning (RP)
	Communications (CO)
	Analysis (AN)
	Mitigation (MI)
	Improvements (IM)
RECOVER (RC)	Recovery Planning (RP)
	Improvements/Gap Remediation (IM)
	Communications (CO)

What processes and assets need protection?

How are we protecting our networks and data?

What are our capabilities for detecting a cyber attack?

What are our capabilities for responding to an attack?

What are our capabilities for returning to normal operations?

Protected Critical Infrastructure Information Program - PCII

Protected Critical Infrastructure Information (PCII) Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
  - Public release under Freedom of Information Act requests,
  - Public release under State, local, tribal, or territorial disclosure laws,
  - Use in civil litigation and
  - Use in regulatory purposes.

Geoff Jenista, CISSP
October 28, 2021

Multi-State Information Sharing Analysis Center (MS-ISAC)

The MS-ISAC mission is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

- All state, local, tribal and territorial governments in the United States are eligible for ***Free*** MS-ISAC membership

- MS-ISAC Members include:
  - All 56 US States and Territories
  - All 78 federally recognized fusion centers
  - More than 5,000 local governments and tribal nations

- Cyber Threat Intelligence
- Emergency Conference Calls
- Network & Web Application Vulnerability Assessments
- Free Access to Tools to Assess your Configuration
- Forensic Analysis, Malware Analysis & Log Analysis
- Reverse Engineering
- Mitigation Recommendations

Geoff Jenista, CISSP
October 28, 2021

Federal Incident Response

Threat Response	Asset Response
Federal Bureau of Investigation (FBI): FBI Field Office Cyber Task Forces: http://www.fbi.gov/contactus/field Internet Crime Complaint Center (IC3): http://www.ic3.gov ▪ Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces. ▪ Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.	**United States Computer Emergency Readiness Team:** http://www.us-cert.gov ▪ Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.
National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center: cywatch@ic.fbi.gov or (855) 292-3937 ▪ Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of Federal law enforcement agencies or the Federal Government.	**The Multi-State Information Sharing and Analysis Center (MS-ISAC)** is a voluntary and collaborative effort designated by the U.S. Department of Homeland Security as the key resource for cyber threat prevention, protection, response and recovery for the nation's State, Local, Tribal, and Territorial governments. **1.866.787.4722** **soc@msisac.org**
United States Secret Service (USSS) Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs): http://www.secretservice.gov/contact/field-offices ▪ Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information.	**Center for Internet Security (CIS)** • Albert Sensors (Intrusion Detection) • Vulnerability Management • Baseline Configuration Guides • Assessment Tools
CISA Central (CENTRAL) (888) 282-0870 or Central@cisa.dhs.gov	

Reporting sites and resources

FBI Reporting
https://www.ic3.gov/

CISA Reporting
https://us-cert.cisa.gov/report

Link to our Cyber Hygiene Services –
https://www.cisa.gov/cyber-hygiene-services

Link to the CISA Website with details –
https://www.cisa.gov/cyber-resource-hub

Link to MS-ISAC –
https://www.cisecurity.org/ms-isac/

Stop Ransomware –
https://www.cisa.gov/stopransomware

Contact Information

Geoffrey F. Jenista, CISSP
Cybersecurity Advisor
Region 7, (IA, KS, MO, NE)
(913) 249-1539
geoffrey.jenista@cisa.dhs.gov

For inquiries or further information,
contact cyberadvisor@dhs.gov