HOMELAND SECURITY PERSPECTIVES FOR BUILDING CYBER SECURITY CAPACITY, CAPABILITY AND RESILIENCE

PATUXENT PARTNERSHIP CONFERENCE – 14 SEPTEMBER 2021

CISA Cybersecurity Advisor Program

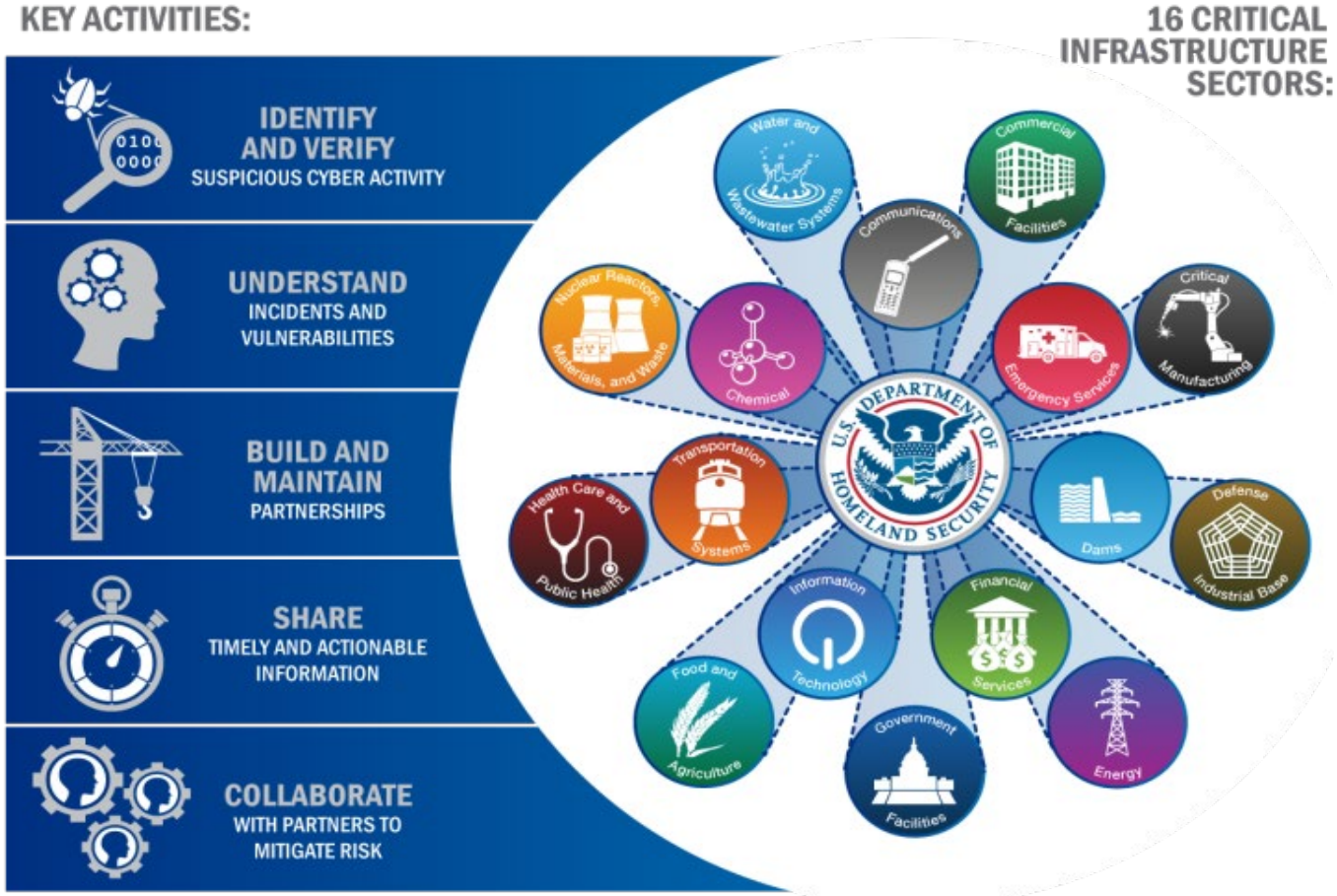
Franco CAPPA, CISSP
Cybersecurity Advisor (CSA)

CISA Mission and Vision

- **Cybersecurity and Infrastructure Security Agency (CISA) mission**:
  - Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure
- **CISA vision**:
  - A Nation with secure, resilient, and reliable critical infrastructure upon which the American way of life can thrive

"***Defend Today, Secure Tomorrow***"

Critical Infrastructure (CI) Sectors

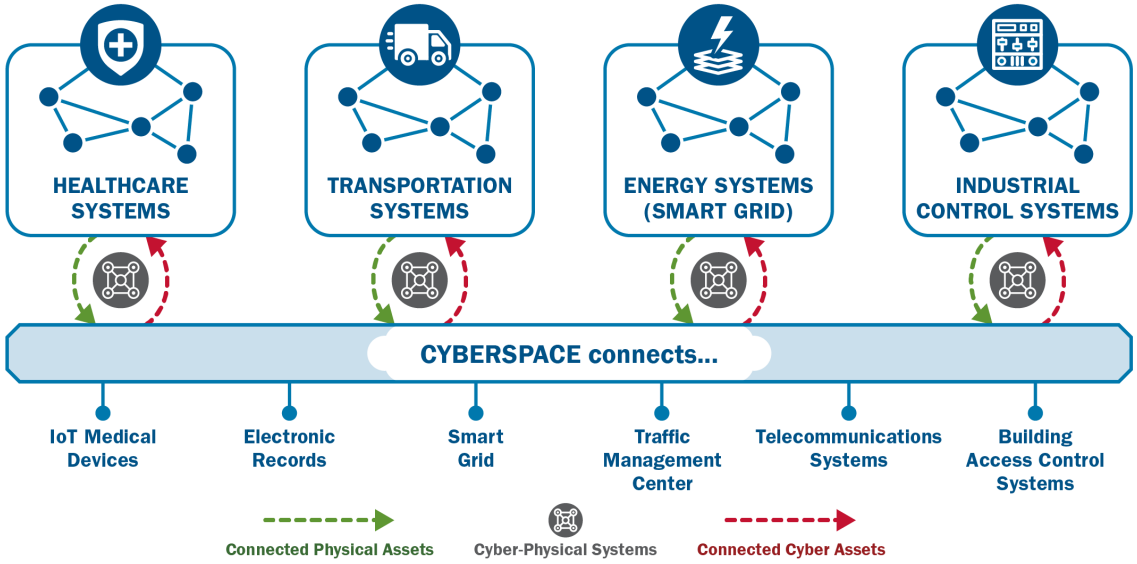


CISA "Pillars" & Field Resources

- **Cybersecurity**--Cybersecurity Advisors (CSAs)
- **Infrastructure Security**—Protective Security Advisors (PSAs) and Chemical Security Inspectors (CSIs)
- **Emergency Communications**—Emergency Communication Coordinators (ECCs)
- **National Risk Management**—Risk analyst

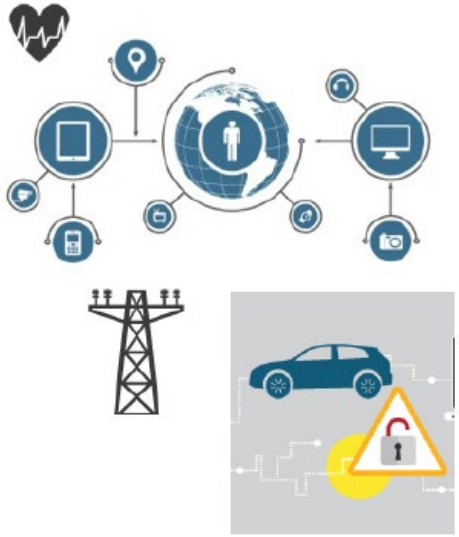
Cyber-Physical Convergence

Today's threats are targeting physical and cyber assets through sophisticated hybrid attacks with potentially devastating impacts to data, property and physical safety. CISA defines convergence as formal collaboration between previously disjoined security functions.



Source: https://www.cisa.gov/cybersecurity-and-physical-security-convergence

Cyber vs Physical



PPD 21 Identifies critical infrastructure as "*interdependent functions and systems in both the physical space and cyberspace*" and aims to strengthen security and resilience "against both the physical and cyber attacks"

A Wide Range of Offerings for CI

Preparedness Activities

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

Offerings for CI—continued

Response Assistance

- Remote / On-Site Assistance
- Malware Analysis
- Hunt and Incident Response Teams
- Incident Coordination

Protective Security Advisors

Five mission areas that directly support the protection of critical infrastructure

1. Plan, coordinate, and conduct security surveys and assessments (i.e., IST, SAFE)
2. Plan and conduct outreach activities
3. Support National Special Security Events (NSSEs) & Special Event Activity Rating (SEAR) events
4. Respond to incidents
5. Coordinate and support improvised explosive device awareness and risk mitigation training

Cyber: A Growing Challenge

Scale

- The number of cyber attacks has never been greater

Sophistication

- Cyber attacks are increasing in complexity

Trends

- Attackers are increasing their advantage

Attack Surface

- Growing volumes of data = more targets

Emerging Cyber Threat Trends

Source: DHS I&A

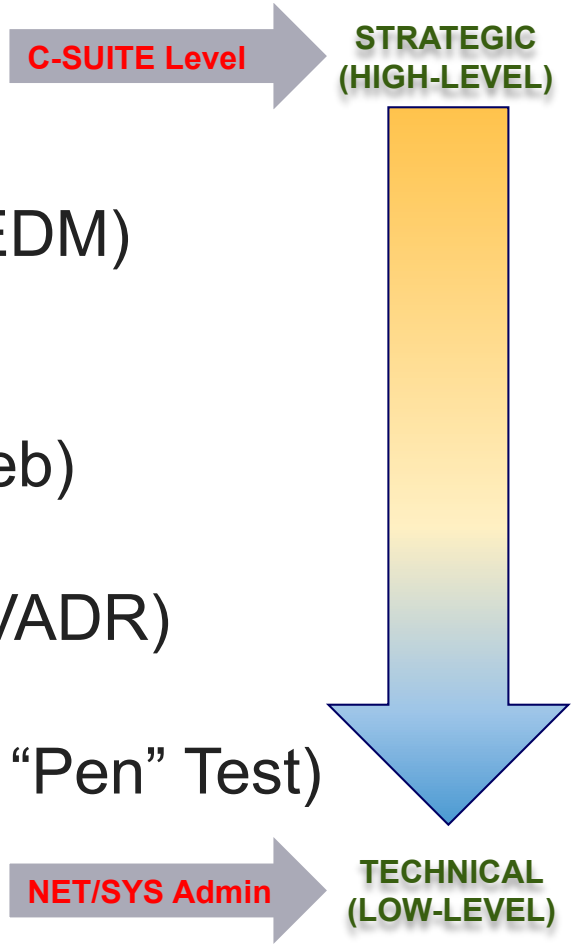
- Interconnected systems enabling threat actors.
  - Targets of opportunity.
  - Paths of least resistance.
- PII and data: high value, high-demand commodities.
- Hacking as a service (HaaS)
  - Malicious tools readily available for purchase or download.

Threat Vectors

- Phishing / Spear-phishing
- Social Engineering
- Business Email Compromise (BEC)
- Exploiting unpatched vulnerabilities on web-facing systems
  - Especially remote-access (e.g., VPN, RDP)
- Exploiting third-parties (e.g., managed services)
- Compromising home networks of employees or family members via emails & telework applications
- Focus on remote / collaboration platforms and cloud services (O365, Webex, Google Drive credentials)

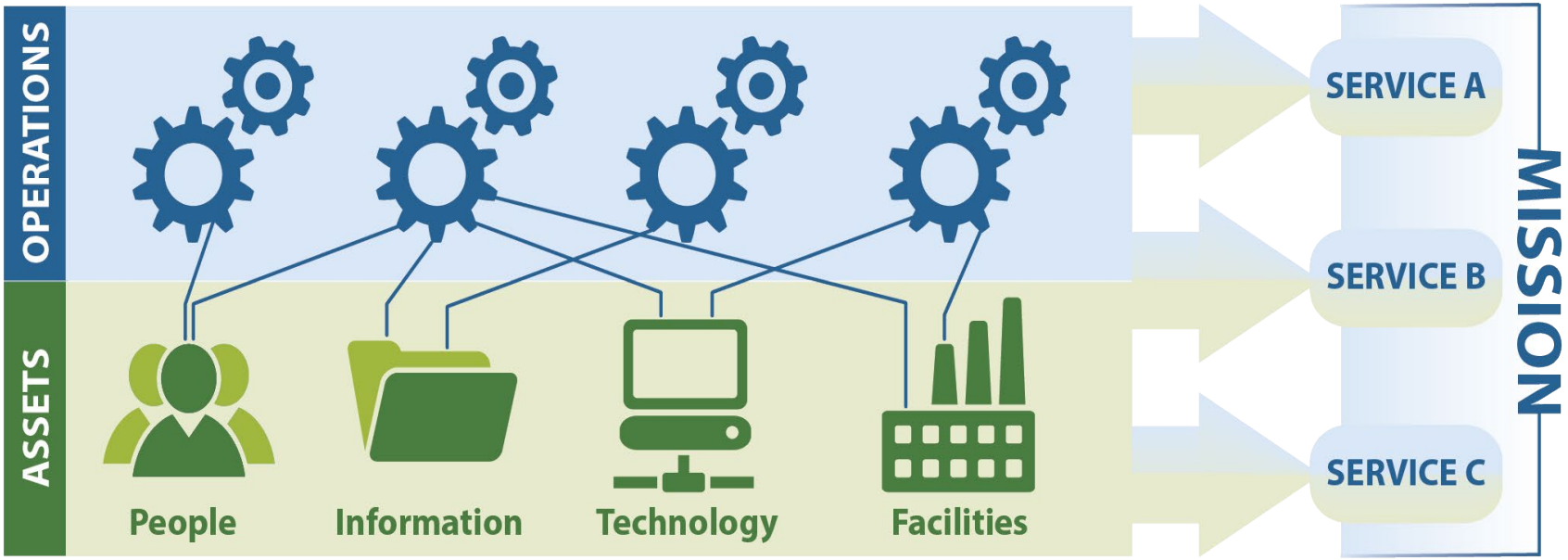
Cybersecurity Assessments

- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)
- Cyber Security Evaluation Tool (CSET)
- Cyber Hygiene Services (Systems & Web)
- Phishing Campaign Assessment
- Validated Architecture Design Review (VADR)
- Remote Penetration Testing (RPT)
- Risk and Vulnerability Assessment (aka “Pen” Test)



Critical Service Focus

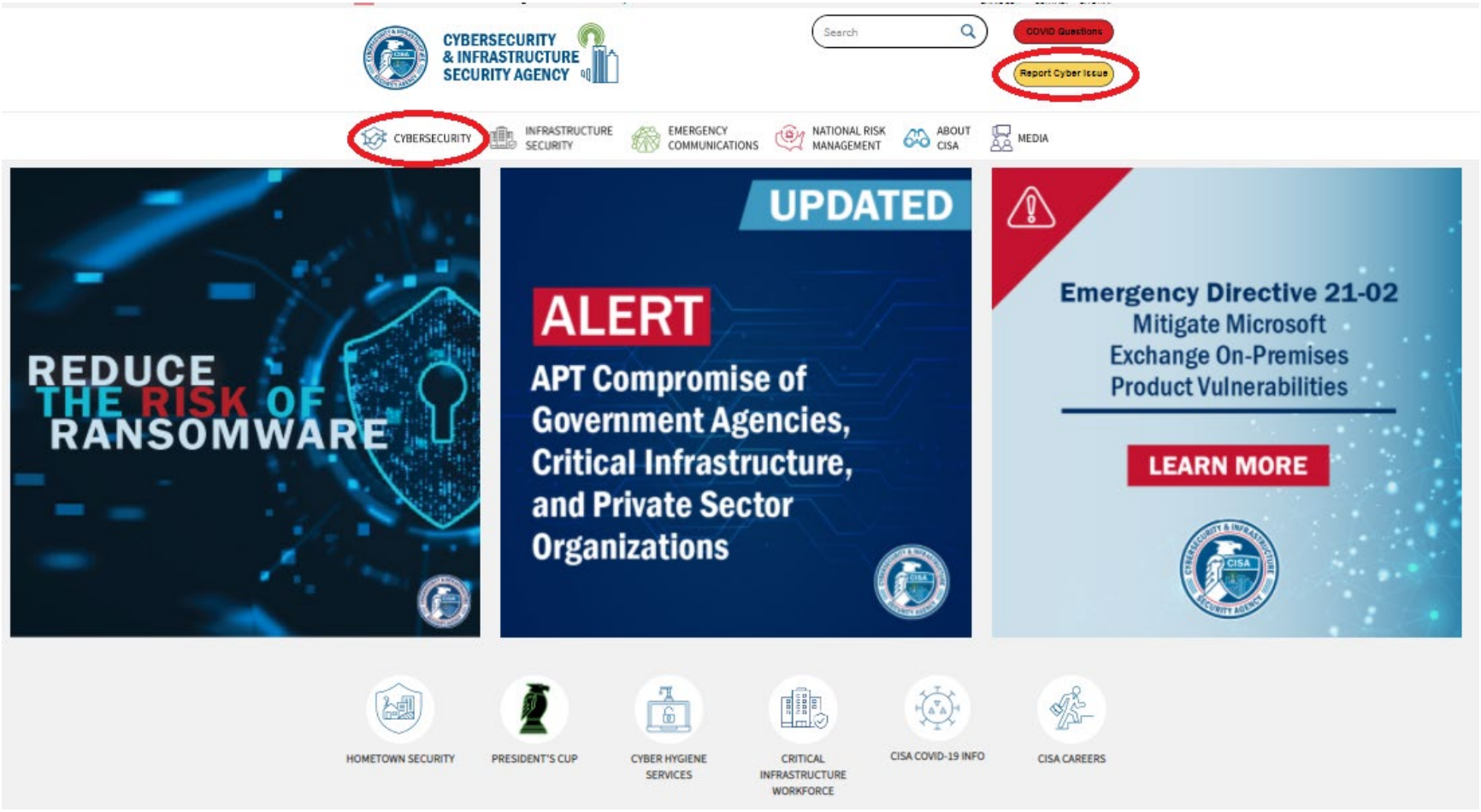
Organizations use **assets** (*people, information, technology, and facilities*) to provide **operational services** and accomplish **missions**.



Cybersecurity Training & Exercises

- **CISA** offers easily accessible education and awareness resources through the **National Initiative for Cybersecurity Careers and Studies** (NICCS) website.
- **FedVTE** is an online, on-demand training center that provides free cybersecurity training for U.S. veterans and federal, state, local, tribal, and territorial government employees
- CISA's **Cybersecurity Training & Exercise** develops, conducts, and evaluates cyber exercises and planning activities for state, local, tribal and territorial governments and public and private sector critical infrastructure organizations.

CISA Resources & Reporting



Integrated CISA Watch

The mission of **CISA Central** is to serve as a national center for reporting of and mitigating communications and incidents.

- Provide alerts, warnings, common operating picture on cyber and communications incidents in real time to virtual and on-site partners
- Work 24X7 with partners to mitigate incidents (On-site partners include the DoD, FBI, Secret Service, Information Sharing and Analysis Centers (ISACs) and other DHS components and public partners)

Federal Cybersecurity Response

PPD 41 Highlights:

- Released in July 2016, sets forth the principles governing the Federal Government's response to any cyber incident. Cybersecurity Act of 2018, landmark legislation that established CISA elevating their mission and authority within the Federal Government.
- Establishes the National Cyber Incident Response Plan and Defines cyber incident and significant cyber incident severity schema scoring.
- CISA National Cyber Incident Scoring System (reference below)

Reference CISA NCISS: https://us-cert.cisa.gov/CISA-National-Cyber-Incident-Scoring-System

Federal Cybersecurity Response

- Established architecture for Federal Government response for to significant cyber incidents through concurrent lines of effort:
  - Asset Response: DHS Cybersecurity and Infrastructure Security Agency (CISA) through what is now CISA Central (Former NCCIC)
  - Threat Response: Department of Justice (DOJ) through the Federal Bureau of Investigation (FBI)
  - Intelligence Support: Office of the Director of National Intelligence (ODNI)
- Codified role and stand-up procedures for Cyber Unified Coordination Group (UCG)

Reference: CISA Insights & CISA.GOV

Federal Incident Response

- **Threat Response:** Attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. Conducting criminal investigations and other actions to counter the malicious cyber activity.
- **Asset Response:** Protecting assets and mitigating vulnerabilities in the face of malicious cyber activity, reducing the impact to systems and data; strengthening, recovering, and restoring services; identifying other entities at risk; and assessing potential risk to broader community.

Key Federal Points of Contact

Threat Response

Federal Bureau of Investigation
855-292-3937 or cywatch@ic.fbi.gov

FBI Field Office Cyber Task Forces
http://www.fbi.gov/contact-us/field

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

U.S. Secret Service
https://www.secretservice.gov/contact/field-offices

Asset Response

CISA Watch
888-282-0870 or central@cisa.dhs.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.

FBI Internet Crime Complaint Center
https://www.ic3.gov/

CISA Mailing Lists and Feeds

- **Alerts** — timely information about current security issues, vulnerabilities, and exploits
- **Analysis Reports** — in-depth analysis on new or evolving cyber threats
- **Bulletins** — weekly summaries of new vulnerabilities. Patch information is provided when available
- **Tips** — advice about common security issues for the general public
- **Current Activity** — up-to-date information about high-impact types of security activity affecting the community at large

Source: US-CERT.gov

Ransomware Threat Overview

- The number of ransomware incidents reported to CISA has steadily increased
- Threat actors are heavily targeting organizations with internet-facing Remote Desktop Protocol (RDP) ports and services
- Threat actors are also leveraging popular phishing malware delivery systems (i.e., Emotet, TrickBot, etc.)
- Adversaries may shift from automated ransomware attacks to human-operated ransomware allowing the threat actors to adapt and change tactics to remain in target networks and more difficult to defend against.

Ransomware Considerations

- Organizations should be aware of and address three areas of concern that can lead to the successful delivery of ransomware:
  - phishing attempts
  - unpatched public-facing systems
  - weak password policy enforcement
- If you fall victim to a ransomware attack, ask for help – reach out to CISA or our FBI and Secret Service colleagues.

Practical Suggestions

- Cyber Hygiene Services
  - Evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts
- Phishing Campaign Assessment
  - Provides an opportunity for determining the potential susceptibility of personnel to phishing attacks. This is a practical exercise intended to support and measure the effectiveness of security awareness training

Practical Suggestions—continued

CSET Ransomware Readiness Assessment (RRA)

- Helps organizations evaluate their cybersecurity posture, with respect to ransomware
- 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 an analysis dashboard with graphs and tables that present the assessment results in both summary and detailed form.

Source: https://github.com/cisagov/cset/releases/tag/v10.3.0.0

CSET RRA—continued

- 10 Goals with 48 tiered practices; 18 Basic, 16 Intermediate, 14 Advanced
- Based off CISA Cyber Essentials, Ransomware Guide and leverages the MITRE ATT&CK Framework
- Structured to give organizations a clear path for improvement
- Complete with supplemental resources for each practice Several types of reports and charts depicting results
- Deficiency report highlighting weakest goals

Source: https://github.com/cisagov/cset/releases/tag/v10.3.0.0

STOP Ransomware Website

Source: https://stopransomware.gov/

Ransomware Guide

RANSOMWARE GUIDE

On September 30, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center released a joint Ransomware Guide, which is a customer centered, one-stop resource with best practices and ways to prevent, protect and/or respond to a ransomware attack. CISA and MS-ISAC are distributing this guide to inform and enhance network defense and reduce exposure to a ransomware attack:

This Ransomware Guide includes two resources:

- **Part 1: Ransomware Prevention Best Practices**
- **Part 2: Ransomware Response Checklist**

Taxonomy Topics: Cybersecurity

Attachment

Ransomware Guide (Sept. 2020) 2.43 MB

Source: https://www.cisa.gov/publication/ransomware-guide

Critical Manufacturing

CRITICAL MANUFACTURING SECTOR SECURITY GUIDE

The Critical Manufacturing Sector Security Guide consolidates effective industry security practices into a framework for Critical Manufacturing owners and operators to select and implement security activities and measures that promote the protection of personnel, public health, public safety, and public confidence. Owners and operators may review the document in full or focus on specific security practice components that address their specific security needs or augment existing security practices. Though Critical Manufacturing Sector security practices are frequently integrated across the enterprise (especially with increasingly converging physical and cyber technologies), they can be organized into four major categories: physical, cyber, personnel, and supply chain. The guide discusses these practices and provides additional information on the various tools, capabilities, and references available to owners and operators.

Taxonomy Topics: Infrastructure Security

Attachment Media

Critical_Manufacturing_Sector_Security_Guide_07012020_1.pdf 2.57 MB

Source: https://www.cisa.gov/publication/critical-manufacturing-sector-security-guide

Securing ICS

SECURING INDUSTRIAL CONTROL SYSTEMS

The Cybersecurity and Infrastructure Security Agency Industrial Control Systems (ICS) strategy, Securing Industrial Control Systems: A Unified Initiative, is a multi-year, focused approach to improve CISA's ability to anticipate, prioritize, and manage national-level ICS risk. Through this "One CISA" initiative, CISA will work with critical infrastructure (CI) owners and operators to build ICS security capabilities that directly empower ICS stakeholders to secure their operations against ICS threats.

The intended audience for CISA's ICS strategy is the whole ICS community and all CISA partners who have an interest in ICS security.

You can find a fact sheet summary of the CISA ICS strategy here.

Taxonomy Topics: Cybersecurity, Infrastructure Security

Attachment Media

Securing Industrial Control Systems	1.82 MB

Source: https://www.cisa.gov/publication/securing-industrial-control-systems

Resources for Midsize and SMB

Resources for Small and Midsize Businesses (SMB)

Cyber Essentials

CISA's Cyber Essentials is a guide for leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices.

Cybersecurity Resources Road Map (A Guide for Critical Infrastructure SMBs)

The Cybersecurity Resources Road Map is a guide for identifying useful cybersecurity best practices and resources based on needs.

Note to cybersecurity trainers and small business advisors:

To professionally print the Cybersecurity Resources Road Map at a print shop (trifold brochure) for distribution to businesses at training events and workshops, use this print shop version of the Road Map and these printing instructions.

Stop.Think.Connect. Toolkit

The Stop.Think.Connect. ™ campaign includes cybersecurity tips for SMBs.

Source: https://us-cert.cisa.gov/resources/smb

CISA Cyber Essentials

CYBER ESSENTIALS TOOLKITS

The Cyber Essentials Toolkit is a set of modules designed to break down the CISA Cyber Essentials into bite-sized actions for IT and C-suite leadership to work toward full implementation of each Cyber Essential. Each chapter focuses on recommended actions to build cyber readiness into the six interrelated aspects of an organizational culture of cyber readiness.

Expand All Sections

Chapter Summary

Cyber Essentials FedVTE Course

Taxonomy Topics: Cybersecurity

Attachment Media

CISA Cyber Essentials Toolkit Chapter 1: Yourself, The Leader	333.35 KB
CISA Cyber Essentials Toolkit Chapter 2: Your Staff, The Users	306.42 KB
CISA Cyber Essentials Toolkit Chapter 3: Your Systems, What Makes You Operational	278.9 KB
CISA Cyber Essentials Toolkit Chapter 4: Your Surroundings, The Digital Workplace	401.63 KB
CISA Cyber Essentials Toolkit Chapter 5: Your Data, What The Business Is Built On	387.73 KB
CISA Cyber Essentials Toolkit Chapter 6: Your Crisis Response	339.6 KB

Source: https://www.cisa.gov/publication/cyber-essentials-toolkits

Telework Essentials Toolkit

TELEWORK ESSENTIALS TOOLKIT

The Telework Essentials Toolkit is designed to assist business leaders, IT staff, and end users in their transition to a secure, permanent telework environment through simple, actionable recommendations. The Toolkit provides three personalized modules for executive leaders, IT professionals, and teleworkers. Each module outlines distinctive security considerations appropriate for their role:

- Actions for executive leaders that drive cybersecurity strategy, investment and culture
- Actions for IT professionals that develop security awareness and vigilance
- Actions for teleworkers to develop their home network security awareness and vigilance

Taxonomy Topics: Infrastructure Security

Attachment

Telework Essentials Toolkit 250.61 KB

Source: https://www.cisa.gov/publication/telework-essentials-toolkit

For more information:
cisa.gov

Questions?
General: CyberAdvisor@cisa.dhs.gov

CSA: franco.cappa@cisa.dhs.gov
PSA: David.Johnston@hq.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY