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

Franco CAPPA, CISSP
Cybersecurity Advisor (CSA)

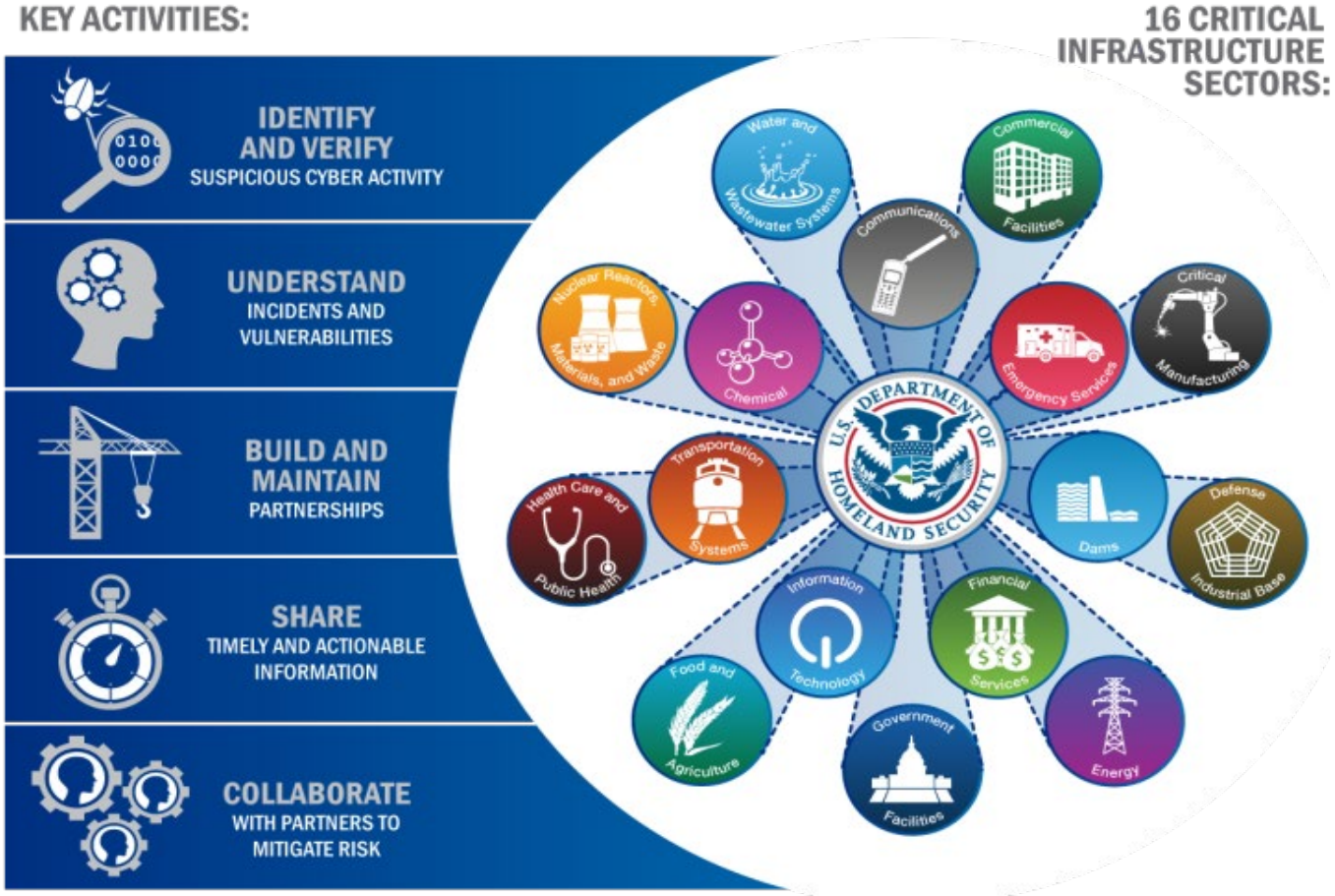
CISA is born …

On **November 16, 2018**, President Trump signed into law the **Cybersecurity and Infrastructure Security Agency Act of 2018**. This landmark legislation elevated the mission of the former National Protection and Programs Directorate (NPPD) within DHS and established CISA.

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

Critical Infrastructure (CI) Sectors



Recent Activities and Alerts

- 12 June 2020 (FBI Notification) — Unattributed Cyber Actors Register Domains Spoofing Legitimate Airport Websites as a Possible Precursor to Future Operational Activity
- 16 July 2020 (Joint NSNC, CSA, NSA, CISA) — APT29 (also known as ‘the Dukes’ or ‘Cozy Bear’). The group uses a variety of tools and techniques to predominantly target governmental, diplomatic, think-tank, healthcare and energy targets for intelligence gain.

Healthcare Report

"A significant uptick in the transition to a remote workforce provides a novel set of highly valuable assets for malicious actors to target. The prevalence of COVID-19 disinformation originating from multiple vectors introduced new unique phishing lures presenting unique challenges to organizations. Finally, the destructive power of ransomware and the threat of data leaks continues to directly disrupt and cause harm to operations within the healthcare sector."

Source: Cybersecurity Trends and Threats for the Healthcare Sector (PERCH – H-ISAC Q2-2020)

Disinformation Campaigns

- Create a lack of trust by U.S. citizens in their government (i.e., Disinformation referenced as fact today)
- Blamed the United States Government (USG) for the creation of the AIDs, SARs, and Ebola epidemics.
- Flooding of stories “amplified” in social media
- Chinese propaganda news amplifies U.S. conspiracy theorist

Emergency Directive

Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to “issue an emergency directive … for the purpose of protecting the information system from, or mitigating, an information security threat.”

Emergency Directive 2020

- Emergency Directive 20-02 on January 14, 2020– Elliptic Curve Cryptography (ECC) certificates and how Windows handles connection requests in the Remote Desktop Protocol (RDP) server and client.
- Emergency Directive 20-03 on July 14, 2020—A remote code execution vulnerability exists in how Windows Server is configured to run the Domain Name System (DNS) Server role.

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

Advisory capabilities (i.e., cyber, physical, emergency communication, etc.)

National Critical Functions

- National Critical Functions are functions of government and the private sector that are so vital to the United States that disruption, corruption, or dysfunction would have a debilitating effect security, national economic security, national public health or safety, or any combination thereof.
- CISA works in close coordination with other federal agencies, the private sector and other key stakeholders in the critical infrastructure community to Identify, Analyze, Prioritize, and Manage the most strategic risks to the Nation's critical infrastructure.

Cybersecurity Advisor (CSA)

CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure.

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess**: Assess critical infrastructure cyber risk.
- **Promote**: Promote best practices and risk mitigation.
- **Build**: Initiate, build capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Educate and raise awareness.
- **Listen:** Collect stakeholder requirements.
- **Coordinate:** Coordinate incident support

Criticality of Periodic Assessments

- Periodic assessments are essential for resilience
- Can’t protect if you don’t know what needs protection
- Can’t fix what needs if you don’t know what’s wrong

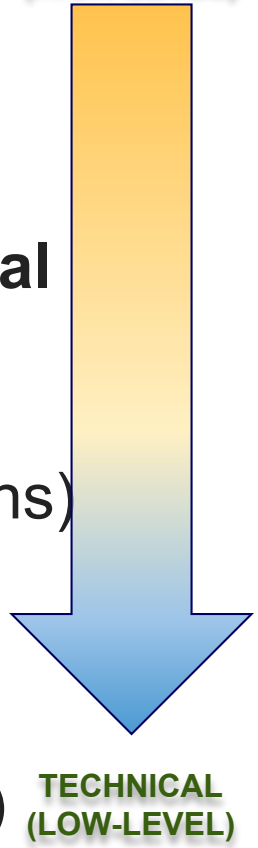
Cybersecurity Assessments

Facilitated Cyber Security Evaluations

- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)

National Cybersecurity Assessments and Technical Services (NCATS) Evaluations

- Cyber Security Evaluation Tool (CSET)
- Cyber Hygiene Service (Network & Web Applications)
- Phishing Campaign Assessment
- Validated Architecture Design Review (VADR)
- Remote Penetration Testing (RPT)
- Risk and Vulnerability Assessment (aka “Pen” Test)



CISA Resources & Reporting

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

CISA 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.

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

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 **National Cyber Exercise and Planning Program (NCEPP)** develops, conducts, and evaluates cyber exercises and planning activities for state, local, tribal and territorial governments and public and private sector critical infrastructure organizations.

Information sharing

Automated Indicator Sharing (AIS) enables the bidirectional sharing of IOCs between the Federal Government and AIS partners in real-time by leveraging industry standards for machine-to- machine communication.

Information Sharing and Analysis Centers (ISACs) and **ISAOs** are non-profit, member-driven organizations for facilitating sharing information between government and industry.

Fusion Centers are state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat.

Integrated CISA Watch

The mission of the **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)

Incident Report/Response/Hunt

CISA Central works to reduce the risk of systemic cybersecurity and communications challenges in our role as the Nation's flagship cyber defense, incident response, and operational integration center.

CISA's Hunt and Incident Response Team (HIRT)

- Provides expert intrusion analysis and mitigation guidance to clients who lack the ability to respond to a cyber incident in-house or require additional assistance.
- Supports federal departments and agencies, state and local governments, the private sector (such as, industry and CI asset owners and operators), academia, etc..

Federal Incident Response

Threat Response	Asset Response
Federal Bureau of Investigation **855-292-3937 or cywatch@ic.fbi.gov**	**CISA Central** 888-282-0870 or NCCICcustomerservice@hq.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.
U.S. Secret Service **secretservice.gov/contact/field-offices**	
Immigration and Customs Homeland Security Investigations **866-347-2423 or ice.gov/contact/hsi**	**Report Internet Crimes**: FBI Internet Crime Complaint Center ic3.gov

Telework Tips

- Do not telework in a public setting
- Be aware of your teleworking environment
- Ensure your laptop and/or smart phone are secured and within your control at all times
- Do not work in a location where your screen may be visible to others
- When discussing critical information, ensure virtual assistants, such as Siri, Alexa and Google Assistant and other internet-connected devices will not pick up your conversations.
- Protect against “shoulder surfing” or eavesdropping
- Consider avoiding using public hotspots or networks

For more information:
cisa.gov

Questions?

General: CyberAdvisor@cisa.dhs.gov
CSA: franco.cappa@cisa.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY