# DHS RESPONSE TO THE 21ST CENTURY THREATS


CISA
CYBER+INFRASTRUCTURE

# CISA is born …

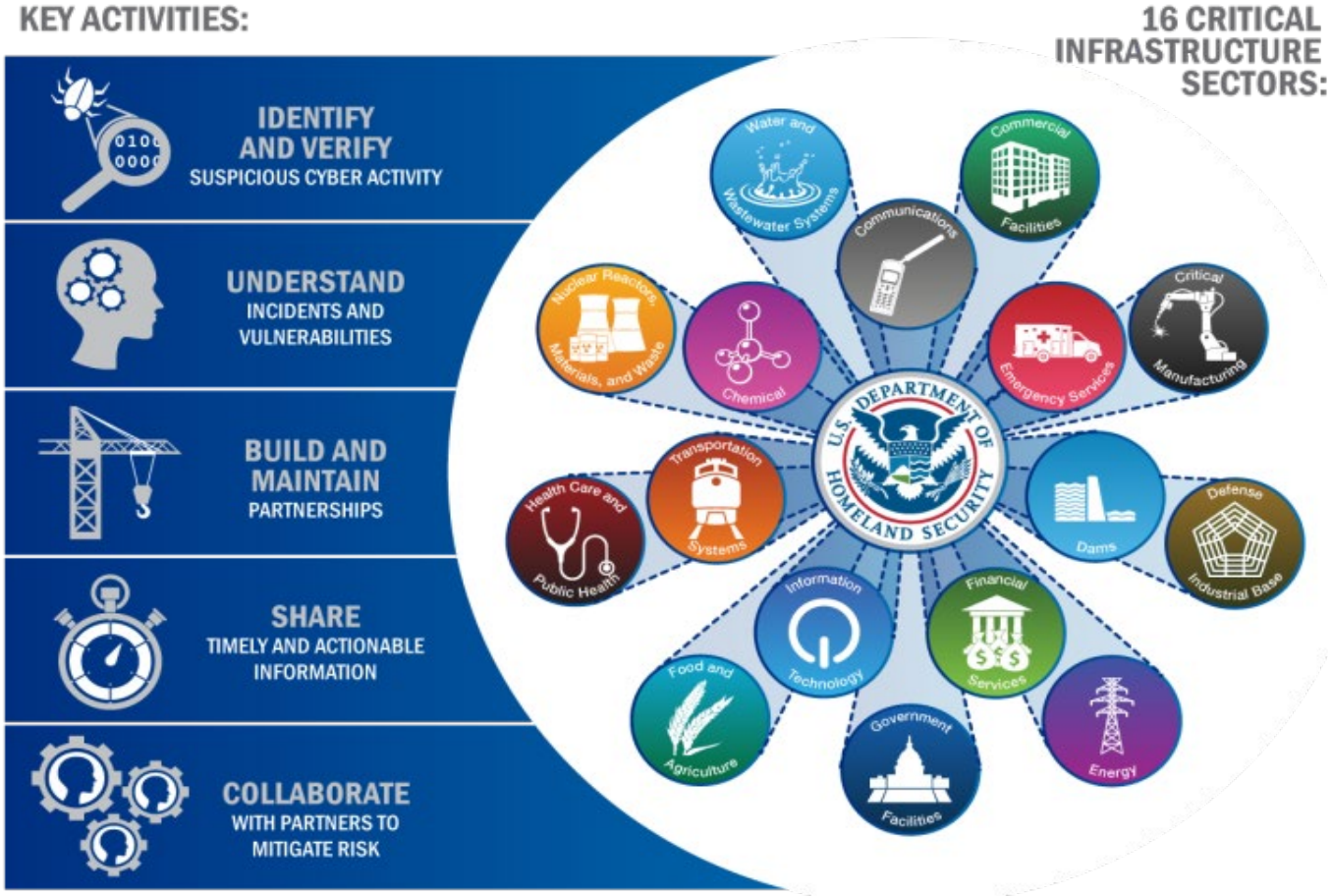
On **November 16, 2018**, President Trump signed into law the **Cybersecurity and Infrastructure Security Agency Act of 2018**. This landmark legislation elevated the mission of the former National Protection and Programs Directorate (NPPD) within DHS and established CISA.

CISA
CYBER+INFRASTRUCTURE

# 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




CISA
CYBER+INFRASTRUCTURE

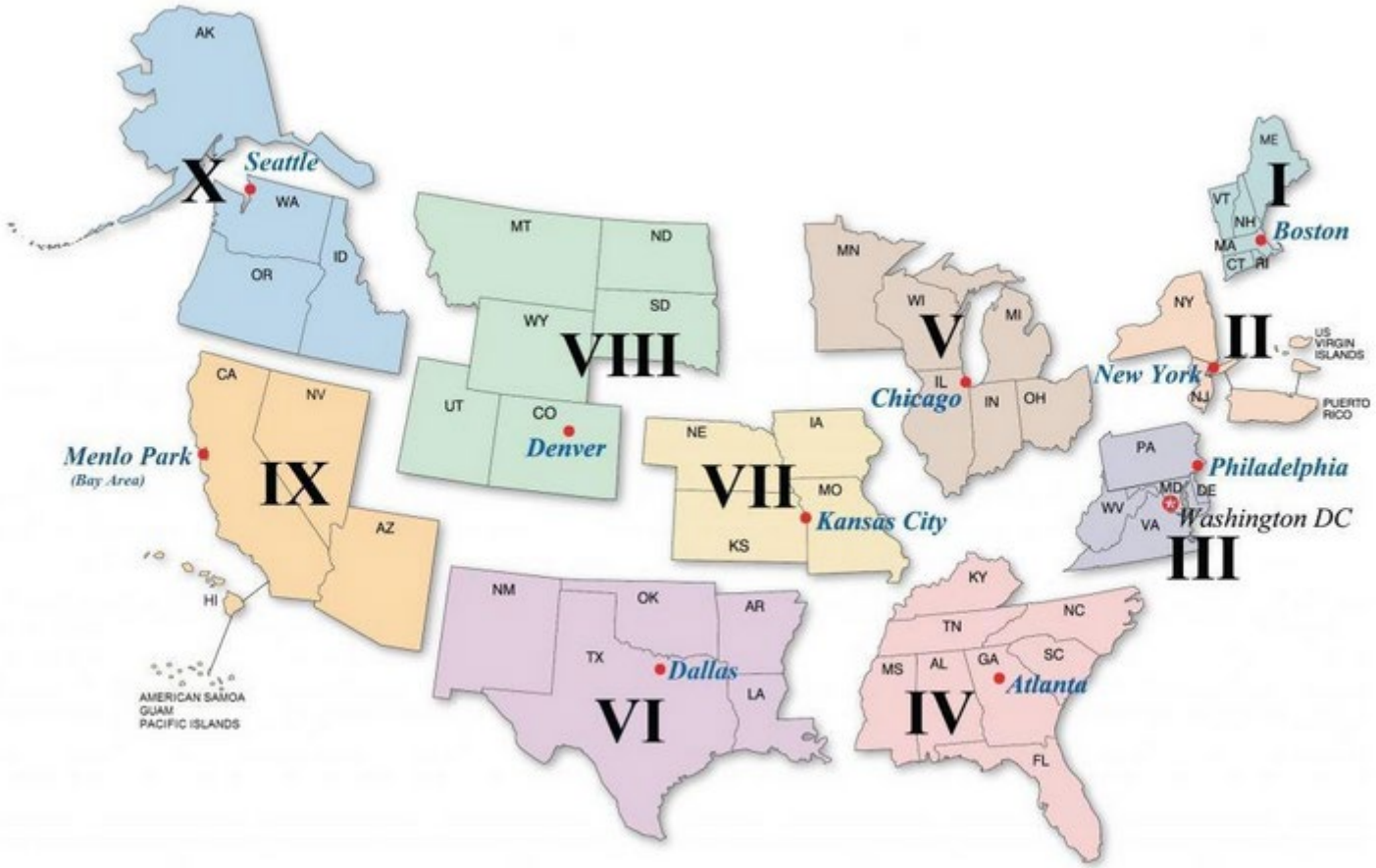
# PCII Program 2002

**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.

CISA
CYBER+INFRASTRUCTURE

# CISA Regional Structure




CISA
CYBER+INFRASTRUCTURE

# What Does CISA Do?

**CISA is responsible for protecting the Nation's critical infrastructure from physical and cyber threats.**

- Cyber Protection
- Infrastructure Resilience
- Emergency Communications
- National Risk Management Center

CISA
CYBER+INFRASTRUCTURE

# Cyber Protection

- CISA's National Cybersecurity and Communications Integration Center (NCCIC) provides 24x7 cyber situational awareness, analysis, incident response and cyber defense capabilities to the Federal government; state, local, tribal and territorial governments; the private sector and international partners.
- CISA provides cybersecurity tools, incident response services and assessment capabilities to safeguard the networks that support the essential operations of federal civilian departments and agencies.

# Infrastructure Resilience

- CISA coordinates security and resilience efforts using trusted partnerships across the private and public sectors, and delivers training, technical assistance, and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide.
- CISA provides consolidated all-hazards risk analysis for U.S. critical infrastructure through the National Risk Management Center.

# Emergency Communications

- CISA enhances public safety interoperable communications at all levels of government, providing training, coordination, tools and guidance to help partners across the country develop their emergency communications capabilities.
- Working with stakeholders across the country, CISA conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters.

# National Risk Management Center

- The NRMC is a planning, analysis, and collaboration center working to identify and address the most significant risks to our nation's critical infrastructure.
- The NRMC works in close coordination with the private sector and other key stakeholders in the critical infrastructure community to: Identify; Analyze; Prioritize; and Manage the most strategic risks to our National Critical Functions.

# National Risk Assessment

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

## DHS National Risk Management Center

The Center will be a government and industry partnership to coordinate risk management efforts, initially by leading a series of activities that will help define what is truly critical; create the frameworks by which government and industry collectively manage risk; and initiate specific cross-sector activities to address known threats.

- Cyber Risk
- Physical Risk
- National Critical Functions
- Integrated Cross-Sector Risk Management Activities
- Analysis and Modeling during Major Incidents

CISA
CYBER+INFRASTRUCTURE

# 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.

# CISA Risk Management Process

**Identify**

- Publish National Critical Functions (public and private stakeholder) groups connected by functions

**Analyze**

- Engage with stakeholders to conduct risk analysis (interdependencies)

**Prioritize**

- Use risk and scenario analysis to build Risk Register

**Manage**

- Convene teams to develop collaborative strategies and implementation plans

# Partnership Development

CISA works with public sectors, 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.

# 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"


CISA CYBER+INFRASTRUCTURE

# U.S. Grid Cyberattack

- Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors (Original release date: March 15, 2018 | Last revised: March 16, 2018)

- March 5, 2019

"A first-of-its-kind cyberattack on the U.S. grid created blind spots at a grid control center and several small power generation sites in the western United States".

Source: eenews.net

CISA CYBER+INFRASTRUCTURE

# Election Security

- Fair and free elections are a hallmark of American democracy. The American people's confidence in the value of their vote is principally reliant on their confidence in the security and resilience of the infrastructure that makes the Nation's elections possible. Accordingly, an electoral process that is both secure and resilient is a vital national interest and one of CISA's highest priorities.
- CISA is committed to working collaboratively with those on the front lines of elections [Physical and Cyber].

Source: https://www.dhs.gov/cisa/election-security



CISA
CYBER+INFRASTRUCTURE

# Cyberspace

- Automation, technology, and network communications have become increasingly essential to our daily lives.
- The amount of information and data stored electronically has grown.
- There is a vast interconnectedness of relationships and dependencies (e.g., government, private sector, third-party)
- As a result, **the country is dependent on the cyber resilience of its critical infrastructure**, such as, the power grid, banking and financial systems, telecommunications, etc..

CISA
CYBER+INFRASTRUCTURE

# Cybersecurity Landscape

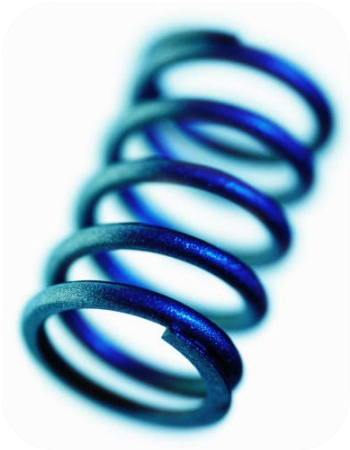
- Cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015 (i.e., damage and destruction of data, lost productivity, restoration, reputational harm, etc.).
- 6 billion Internet users by 2022 (75% of the projected world population) and more than 7.5 billion Internet users by 2030 (90% of the projected world population of 8.5 billion, 6 years of age and older).

Source: Cybersecurity Ventures

# What Is Cyber 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 -- February 12, 2013



| | |
|---|---|
| **Protect (Security)** | **Sustain (Continuity)** |
| **Perform (Capability)** | **Repeat (Maturity)** |

CISA
CYBER+INFRASTRUCTURE

# 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

**Cybersecurity Advisors**

**Protective Security Advisors**

# 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

# Protective Security Advisor (PSA)

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

In support of that mission: Protective Security Advisors (PSAs):

- Plan, coordinate, and conduct surveys & assessments.
- Plan and conduct outreach activities.
- Support national special security events
- Respond to incidents.
- Coordinate and support improvised explosive device awareness and risk mitigation training

CISA
CYBER+INFRASTRUCTURE

# Operational Resilience in Practice

Operational resilience emerges from what we do, such as:

- Identifying and mitigating risks,
- Planning for and managing vulnerabilities and incidents,
- Performing service-continuity processes and planning,
- Managing IT operations,
- Managing, training, & deploying people,
- Protecting and securing important assets, and
- Working with external partners.


CISA
CYBER+INFRASTRUCTURE

# 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

# 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.

# Federal IR—Example

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

CISA CYBER+INFRASTRUCTURE

# NCSAM

- Held every October, **National Cybersecurity Awareness Month (NCSAM)** is a collaborative effort between government and industry to raise awareness about the importance of cybersecurity and to ensure that all Americans have the resources they need to be safer and more secure online.

CISA
CYBER+INFRASTRUCTURE

# NCSAM—continued

- NCSAM 2019 will emphasize personal accountability and stress the importance of taking proactive steps to enhance cybersecurity at home and in the workplace.
- This year's overarching message – **Own IT. Secure IT. Protect IT.**

# Campaign Background

- In 2009, President Obama recognized the need to increase education and dialogue about cybersecurity, as called for in the Cyberspace Policy Review. As part of this policy review, the Department of Homeland Security (DHS) was asked to create an ongoing cybersecurity awareness campaign — **Stop.Think.Connect.™**

# STOP. THINK. CONNECT. - NCSAM

- The **STOP.THINK.CONNECT.™** Campaign is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online.
- **National Cybersecurity Awareness Month (NCSAM)** 2019 will promote personal accountability and encourage proactive behavior to enhance cybersecurity.

# STOP. THINK. CONNECT. Toolkit

- Students K-8, 9-12, and Undergraduate
- Parents and Educators
- Young Professionals
- Older Americans
- Government
- Industry
- Small Business
- Law Enforcement

Source: https://www.dhs.gov/stopthinkconnect-toolkit

CISA
CYBER+INFRASTRUCTURE

# Toolkit Cyber Topics

Social Media Guide

Internet of Things Tip Card

Cybersecurity While Traveling Tip Card

Chatting with Kids about Being Online Booklet

Parents and Educators Tip Card

Mobile Security Tip Card

Seguridad Cibernética Para Los Niños

Best Practices for Creating a Password

Best Practices for Using Public WiFi

Identity Theft and Internet Scams

Mobile Banking and Payments

Online Gaming

Online Privacy

Reporting a Cybercrime Complaint

Insider Threat

Malware

Five Every Day Steps Towards Online Safety

Five Ways to be Cyber Secure at Work

How to Recognize and Prevent Cybercrime

Five Steps to Protecting Your Digital Home

Your Part in Protecting Critical Infrastructure

Phishing

Source: https://www.dhs.gov/stopthinkconnect-toolkit

CISA
CYBER+INFRASTRUCTURE

# It is a shared responsibility!

**STOP. THINK. CONNECT.™**

https://www.dhs.gov/stopthinkconnect

**National Cybersecurity Awareness Month (NCSAM)**

https://www.dhs.gov/national-cyber-security-awareness-month

CISA
CYBER+INFRASTRUCTURE


CISA
CYBER+INFRASTRUCTURE

For more information:
**cisa.gov**

Questions?
**General:** CyberAdvisor@cisa.dhs.gov


# CISA

CYBER+INFRASTRUCTURE