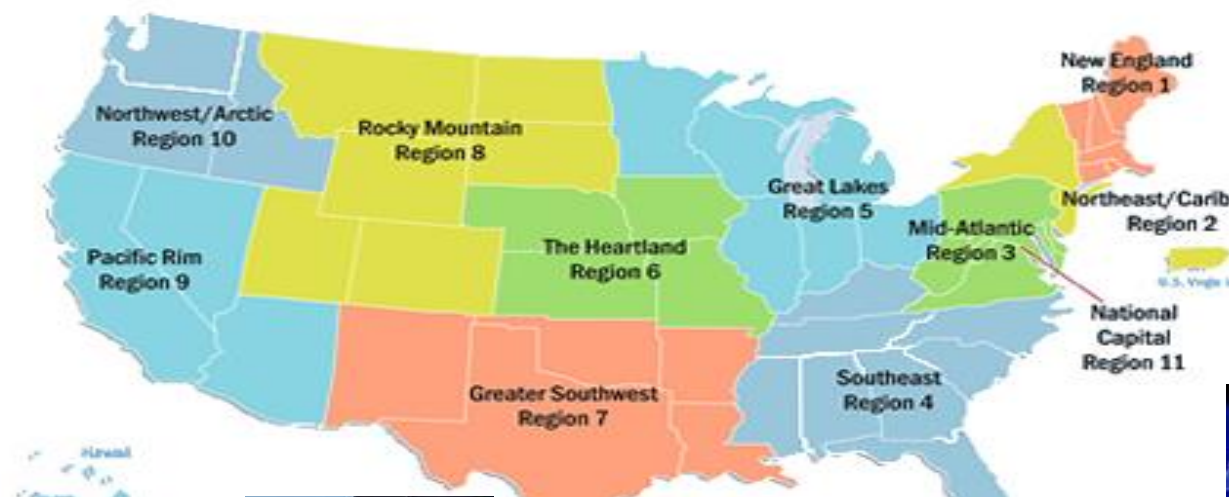
# Critical Infrastructure Sectors and DHS ICS CERT Overview

Presented by Darryl E. Peek II

Homeland Security

UNCLASSIFIED


Alaska
Northwest/Arctic Region 10
Rocky Mountain Region 8
Great Lakes Region 5
New England Region 1
Northeast/Caribbean Region 2
Mid-Atlantic Region 3
Puerto Rico
U.S. Virgin Islands
Pacific Rim Region 9
The Heartland Region 6
National Capital Region 11
Southeast Region 4
Greater Southwest Region 7
Hawaii
Guam

# Authorities and Related Legislation

Homeland Security Act (HSA) (2002)

NSPD-54/ HSPD-23
Cyber Security and Monitoring (2008)

PPD-8
National Preparedness (2011)

PPD-21
Critical Infrastructure Security and Resilience (2013) (supersedes HSPD-7)

EO 13636
Improving Critical Infrastructure Cybersecurity (2013)

FISMA
Federal Information Security Modernization Act (2002/2014)

EO 13691
Promoting Private Sector Cybersecurity Information Sharing (2015)

Cybersecurity Act (2015)

# DHS Mission Alignment

Department of Homeland Security (DHS) Missions

- 1)Prevent terrorism and enhancing security;2)Secure and manage our borders; 3)Enforce and administer our immigration laws; 4)Safeguard and secure cyberspace; 5)Ensure resilience to disasters;

National Protection and Programs Directorate (NPPD) Mission

- The mission of NPPD is to lead the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure.

Office of Cybersecurity & Communications (CS&C) Mission

- Responsible for enhancing the security, resiliency, and reliability of the Nation's cyber and communications infrastructure. CS&C actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets.

# DHS/CS&C Organizational Chart

**Jeh Johnson**
DHS Secretary

Office of the Chief Technology Officer

Enterprise Performance Management Office

**Suzanne Spaulding**
NPPD Undersecretary

**Dr. Phyllis Schneck**
NPPD Deputy Undersecretary

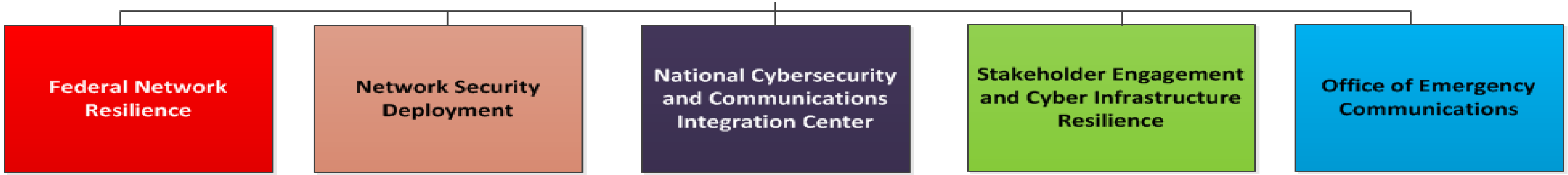
**Dr. Andy Ozment**
CS&C Assistant Secretary

**Gen. Gregory Touhill**
CS&C Dep. Assistant Secretary

**Caitlin Durkovic**
IP Assistant Sec

Office of the Chief of Staff

Office of the General Counsel



Federal Network Resilience

Network Security Deployment

National Cybersecurity and Communications Integration Center

Stakeholder Engagement and Cyber Infrastructure Resilience

Office of Emergency Communications

# Responsibilities

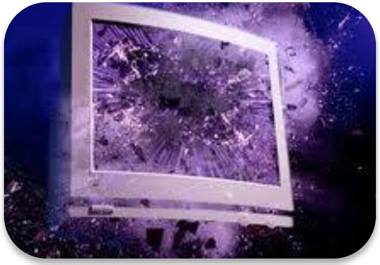
Emergency Communications Capabilities

Secure *dot-gov*

Assist in Protecting *dot-com*

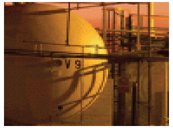
Assist in Securing Critical Infrastructure

National Security Communications

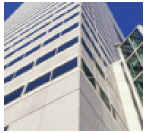


Coordinate Cyber and Communications Incident Response

# Critical Infrastructure Sectors



Chemical



Commercial Facilities

Financial Services

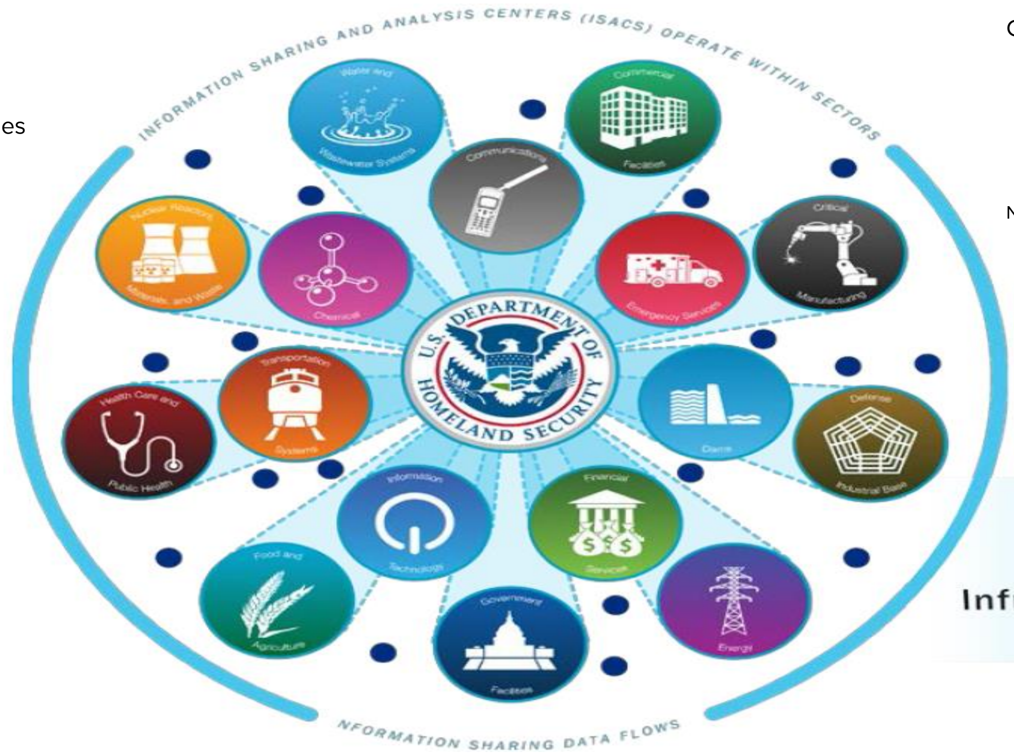
Defense Industrial Base

Dams

Healthcare and Public Health

Transportation Systems

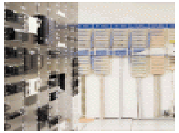
Food and Agriculture


INFORMATION SHARING AND ANALYSIS CENTERS (ISACS) OPERATE WITHIN SECTORS
Water and Wastewater Systems
Commercial Facilities
Communications
Nuclear Reactors, Materials and Waste
Chemical
Emergency Services
Critical Manufacturing
U.S. DEPARTMENT OF HOMELAND SECURITY
Transportation Systems
Health Care and Public Health
Dams
Defense Industrial Base
Information Technology
Financial Services
Food and Agriculture
Government Facilities
Energy
NFORMATION SHARING DATA FLOWS

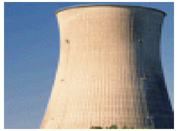
**16 Critical Infrastructure Sectors**

● = Companies

Critical Manufacturing

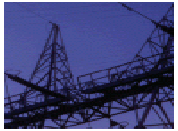


Information Technology

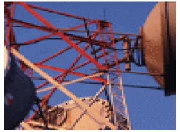


Nuclear Reactors, Materials and Waste

Emergency Services

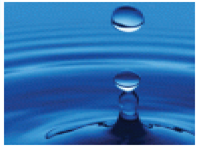


Energy



Communications

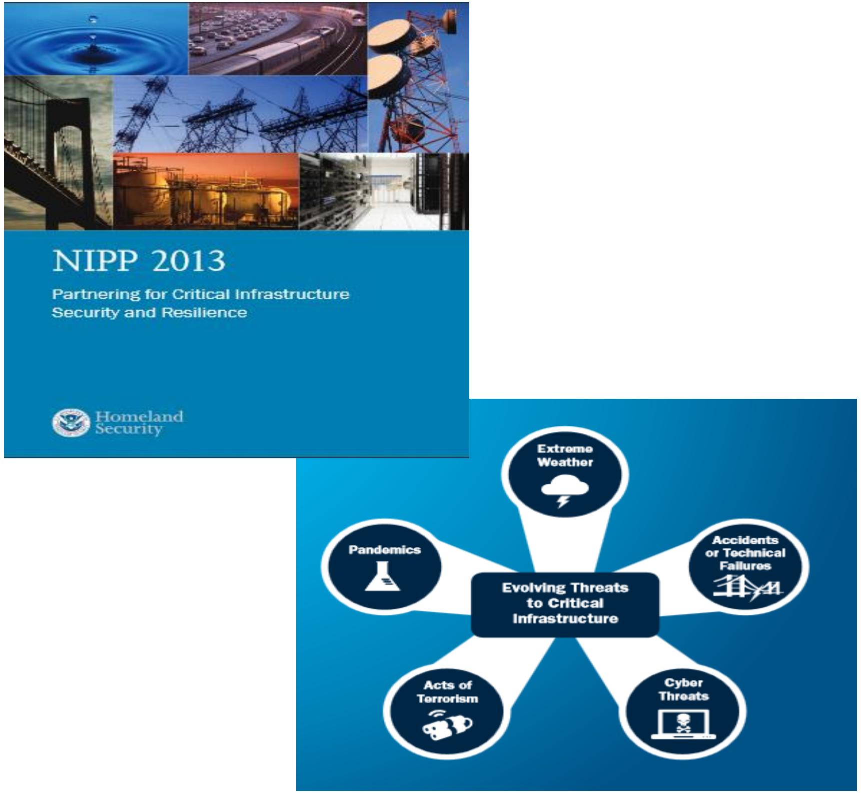
Government Facilities



Water and Wastewater Systems

# National Infrastructure Protection Plan

- 16 Sectors, all different, ranging from asset-focused to systems and networks
- Outside regulatory space
- 85% privately owned
- 100% in State and local jurisdictions



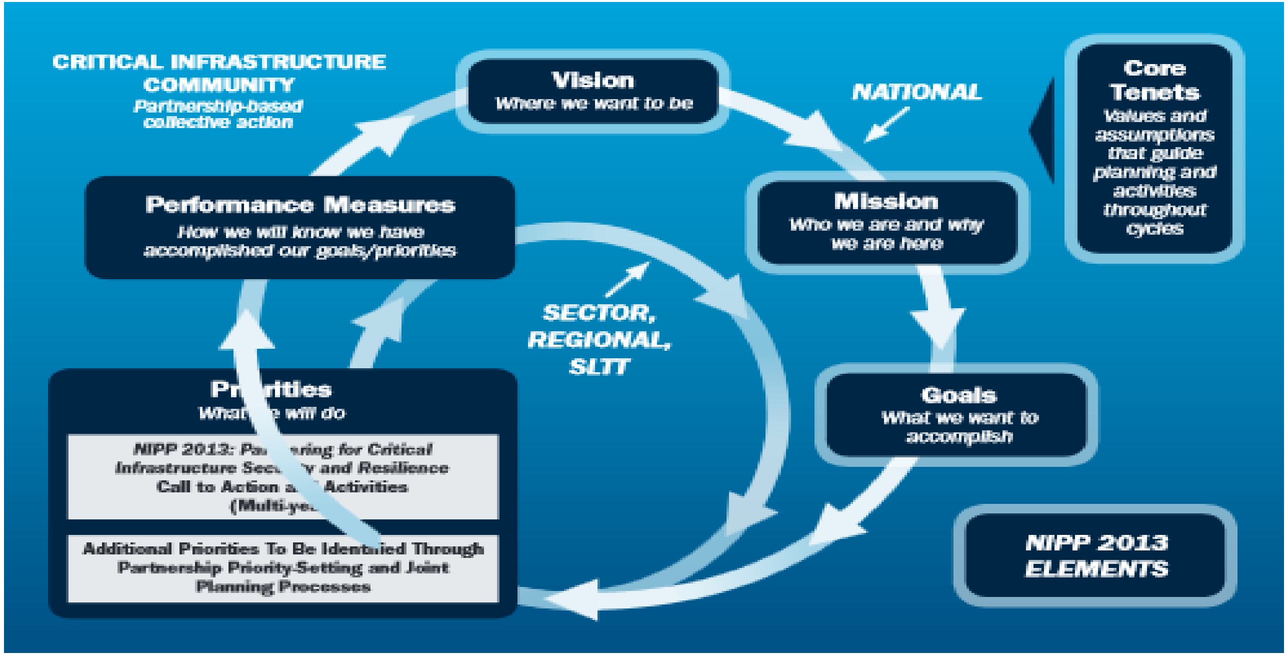
NIPP 2013

Partnering for Critical Infrastructure Security and Resilience

Homeland Security

Extreme Weather
Pandemics
Accidents or Technical Failures
Evolving Threats to Critical Infrastructure
Acts of Terrorism
Cyber Threats

# The National Plan's Approach to Building and Sustaining Unity of Effort



CRITICAL INFRASTRUCTURE COMMUNITY
*Partnership-based collective action*

**Vision**
*Where we want to be*

*NATIONAL*

**Core Tenets**
*Values and assumptions that guide planning and activities throughout cycles*

**Performance Measures**
*How we will know we have accomplished our goals/priorities*

**Mission**
*Who we are and why we are here*

*SECTOR, REGIONAL, SLTT*

**Priorities**
*What we will do*

*NIPP 2013: Partnering for Critical Infrastructure Security and Resilience Call to Action and Activities (Multi-year)*

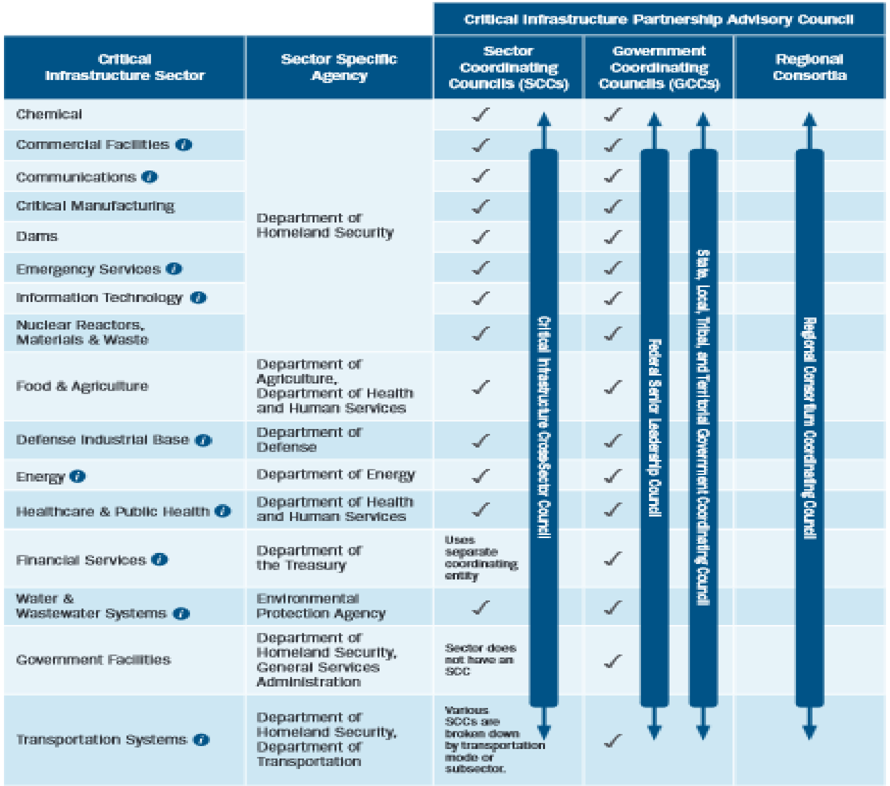
Additional Priorities To Be Identified Through Partnership Priority-Setting and Joint Planning Processes

**Goals**
*What we want to accomplish*

*NIPP 2013 ELEMENTS*

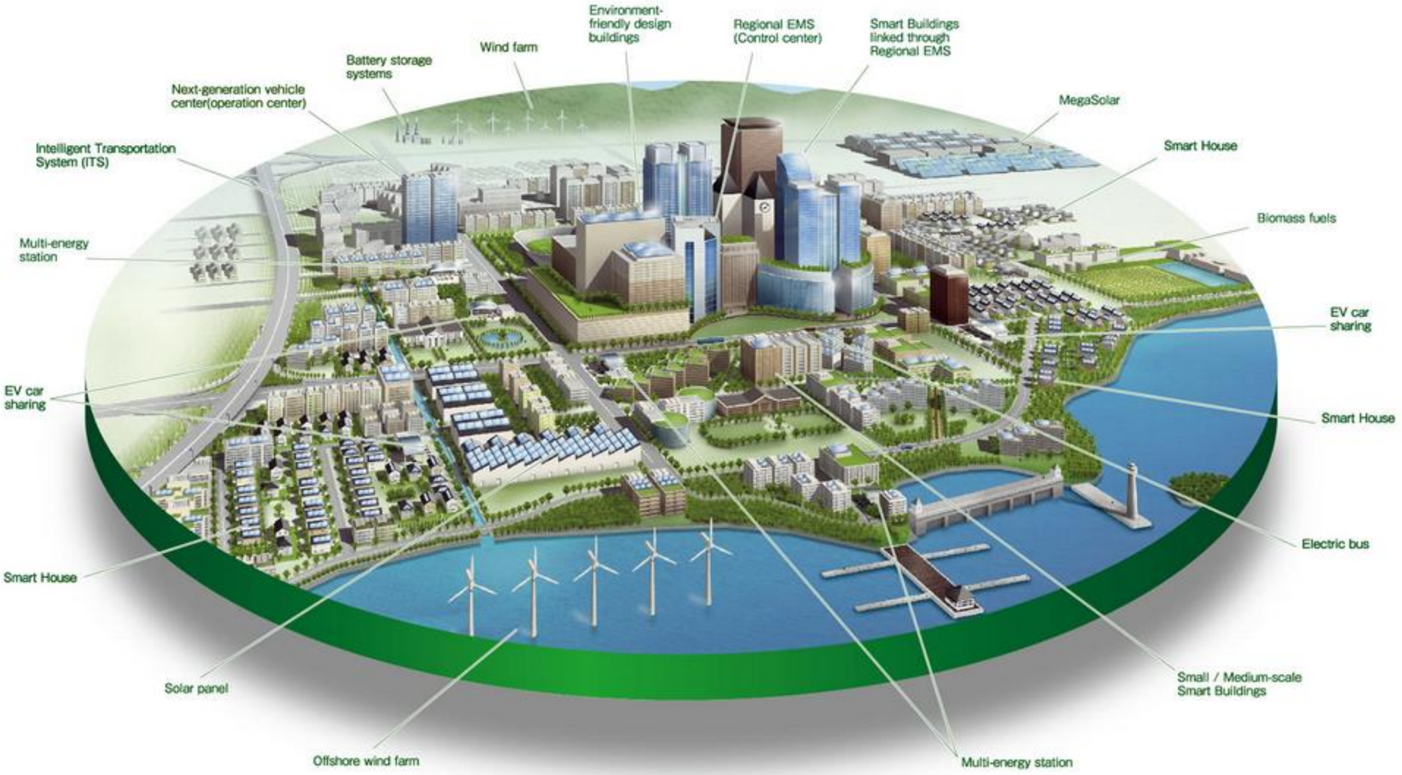
# Sector and Cross Sector Coordinating Councils

- DHS coordinates the overall national effort to enhance CIKR protection and resiliency through the implementation of the NIPP
- Sector-specific agencies lead the activities in each of 16 sectors and develop and implement Sector-Specific Plans
- DHS leads 10 of the sectors
- IP leads six of these sectors



| | | Critical Infrastructure Partnership Advisory Council | | |
|---|---|---|---|---|
| Critical Infrastructure Sector | Sector Specific Agency | Sector Coordinating Councils (SCCs) | Government Coordinating Councils (GCCs) | Regional Consortia |
| Chemical | Department of Homeland Security | ✓<br>Critical Infrastructure Cross-Sector Council | ✓<br>Federal Senior Leadership Council<br>State, Local, Tribal, and Territorial Government Coordinating Council | Regional Consortium Coordinating Council |
| Commercial Facilities | | ✓ | ✓ | |
| Communications | | ✓ | ✓ | |
| Critical Manufacturing | | ✓ | ✓ | |
| Dams | | ✓ | ✓ | |
| Emergency Services | | ✓ | ✓ | |
| Information Technology | | ✓ | ✓ | |
| Nuclear Reactors, Materials & Waste | | ✓ | ✓ | |
| Food & Agriculture | Department of Agriculture, Department of Health and Human Services | ✓ | ✓ | |
| Defense Industrial Base | Department of Defense | ✓ | ✓ | |
| Energy | Department of Energy | ✓ | ✓ | |
| Healthcare & Public Health | Department of Health and Human Services | ✓ | ✓ | |
| Financial Services | Department of the Treasury | Uses separate coordinating entity | ✓ | |
| Water & Wastewater Systems | Environmental Protection Agency | ✓ | ✓ | |
| Government Facilities | Department of Homeland Security, General Services Administration | Sector does not have an SCC | ✓ | |
| Transportation Systems | Department of Homeland Security, Department of Transportation | Various SCCs are broken down by transportation mode or subsector. | ✓ | |

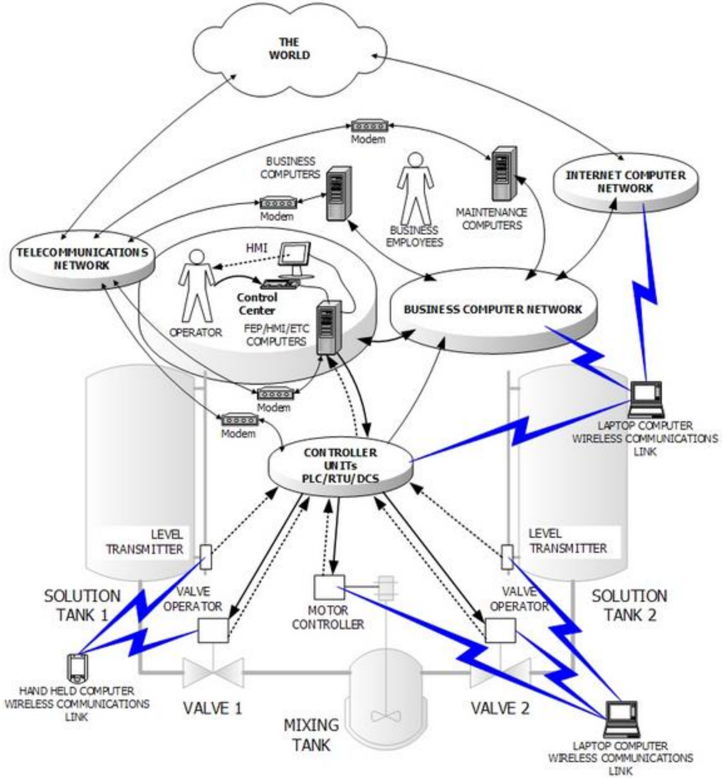
# Tomorrow Land


Environment-friendly design buildings
Regional EMS (Control center)
Smart Buildings linked through Regional EMS
Wind farm
Battery storage systems
Next-generation vehicle center(operation center)
MegaSolar
Intelligent Transportation System (ITS)
Smart House
Biomass fuels
Multi-energy station
EV car sharing
EV car sharing
Smart House
Electric bus
Smart House
Small / Medium-scale Smart Buildings
Solar panel
Offshore wind farm
Multi-energy station

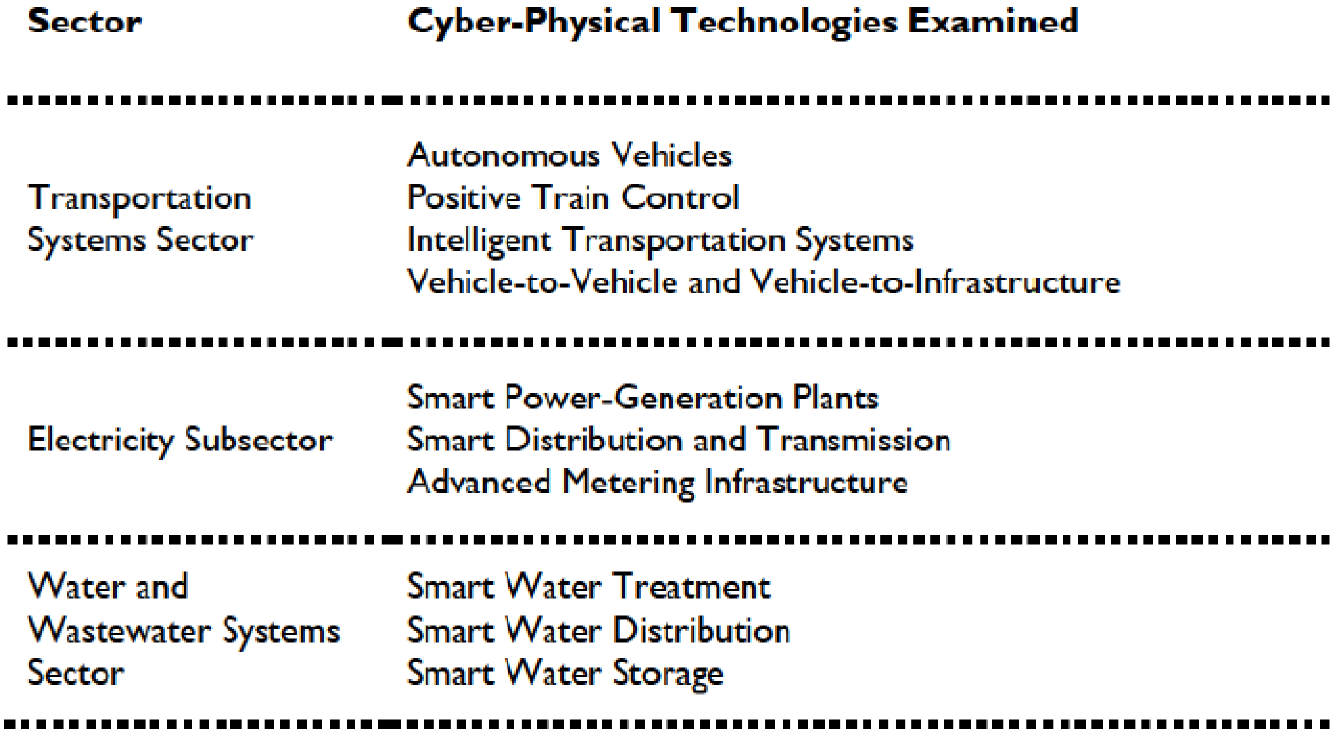
# Vectors to Attack Critical Infrastructure

Attacker Vectors:

- Gain access to the control system LAN
- Through discovery, gain understanding of the process
- Gain control of the process.



# DHS Cyber-Physical Technologies



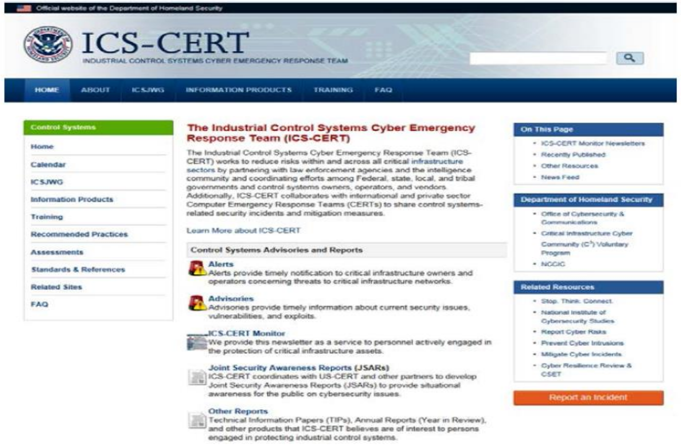
| Sector | Cyber-Physical Technologies Examined |
|---|---|
| Transportation Systems Sector | Autonomous Vehicles<br>Positive Train Control<br>Intelligent Transportation Systems<br>Vehicle-to-Vehicle and Vehicle-to-Infrastructure |
| Electricity Subsector | Smart Power-Generation Plants<br>Smart Distribution and Transmission<br>Advanced Metering Infrastructure |
| Water and Wastewater Systems Sector | Smart Water Treatment<br>Smart Water Distribution<br>Smart Water Storage |

# NCCIC/Industrial Control Systems – Cyber Emergency Response Team (ICS-CERT)

- ICS CERT Watch Floor
- Onsite Incident Response
- Advance Analytical Laboratory
- Cybersecurity Evaluation Tool (CSET)
- Site Assistance and Evaluations
- Outreach and Training
- ICS Joint Working Group
- Strategy for Securing Control Systems

**John Felker**
NCCIC Director

**Marty Edwards**
ICS CERT Director



Official website of the Department of Homeland Security

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Control Systems

- Home
- Calendar
- ICSJWG
- Information Products
- Training
- Recommended Practices
- Assessments
- Standards & References
- Related Sites
- FAQ

**The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)**

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

Learn More about ICS-CERT

**Control Systems Advisories and Reports**

**Alerts**
Alerts provide timely notification to critical infrastructure owners and operators concerning threats to critical infrastructure networks.

**Advisories**
Advisories provide timely information about current security issues, vulnerabilities, and exploits.

**ICS-CERT Monitor**
We provide this newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets.

**Joint Security Awareness Reports (JSARs)**
ICS-CERT coordinates with US-CERT and other partners to develop Joint Security Awareness Reports (JSARs) to provide situational awareness for the public on cybersecurity issues.

**Other Reports**
Technical Information Papers (TIPs), Annual Reports (Year in Review), and other products that ICS-CERT believes are of interest to persons engaged in protecting industrial control systems.

On This Page

- ICS-CERT Monitor Newsletters
- Recently Published
- Other Resources
- News Feed

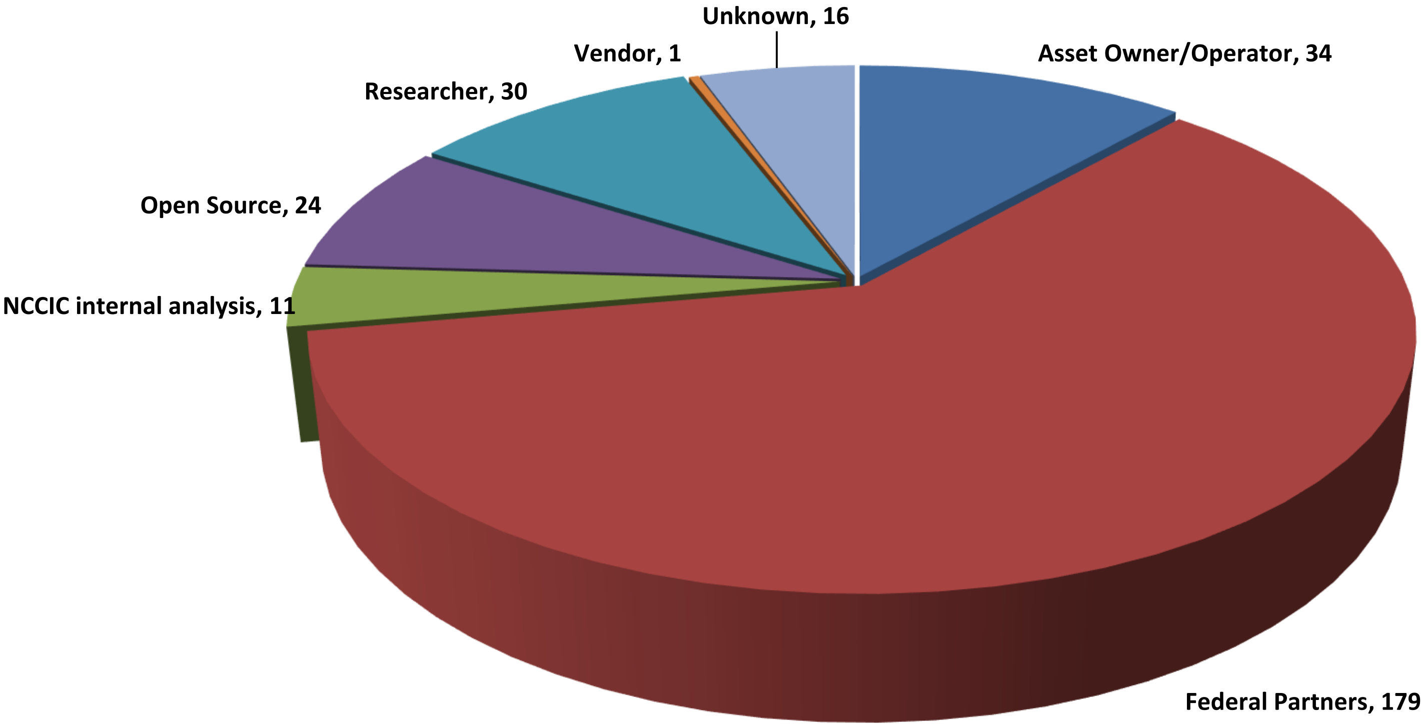
Department of Homeland Security

- Office of Cybersecurity & Communications
- Critical Infrastructure Cyber Community ($C^3$) Voluntary Program
- NCCIC

Related Resources

- Stop. Think. Connect.
- National Institute of Cybersecurity Studies
- Report Cyber Risks
- Prevent Cyber Intrusions
- Mitigate Cyber Incidents
- Cyber Resilience Review & CSET

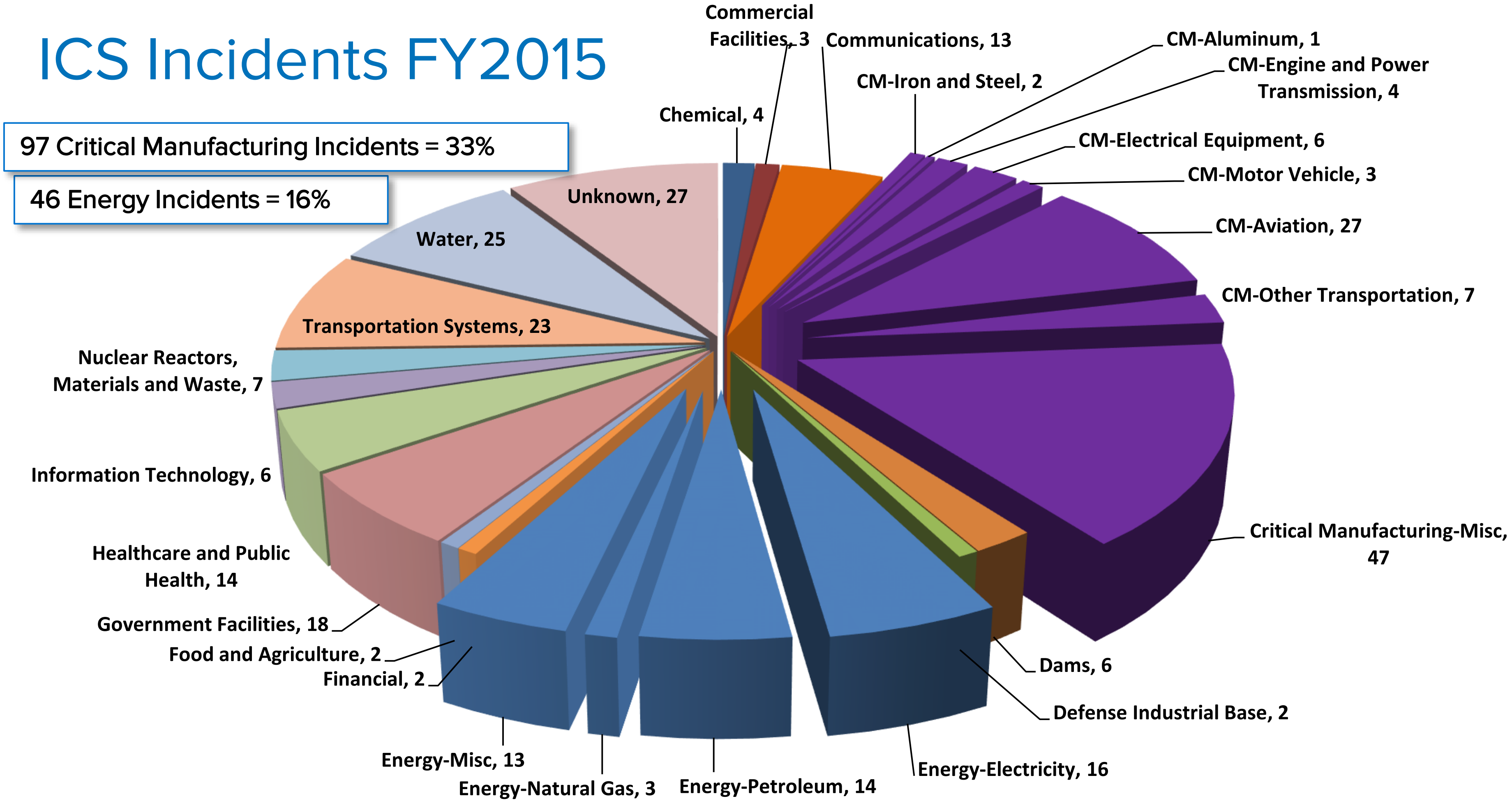
# Fiscal Year 2015 Reporting Source - 295 Total



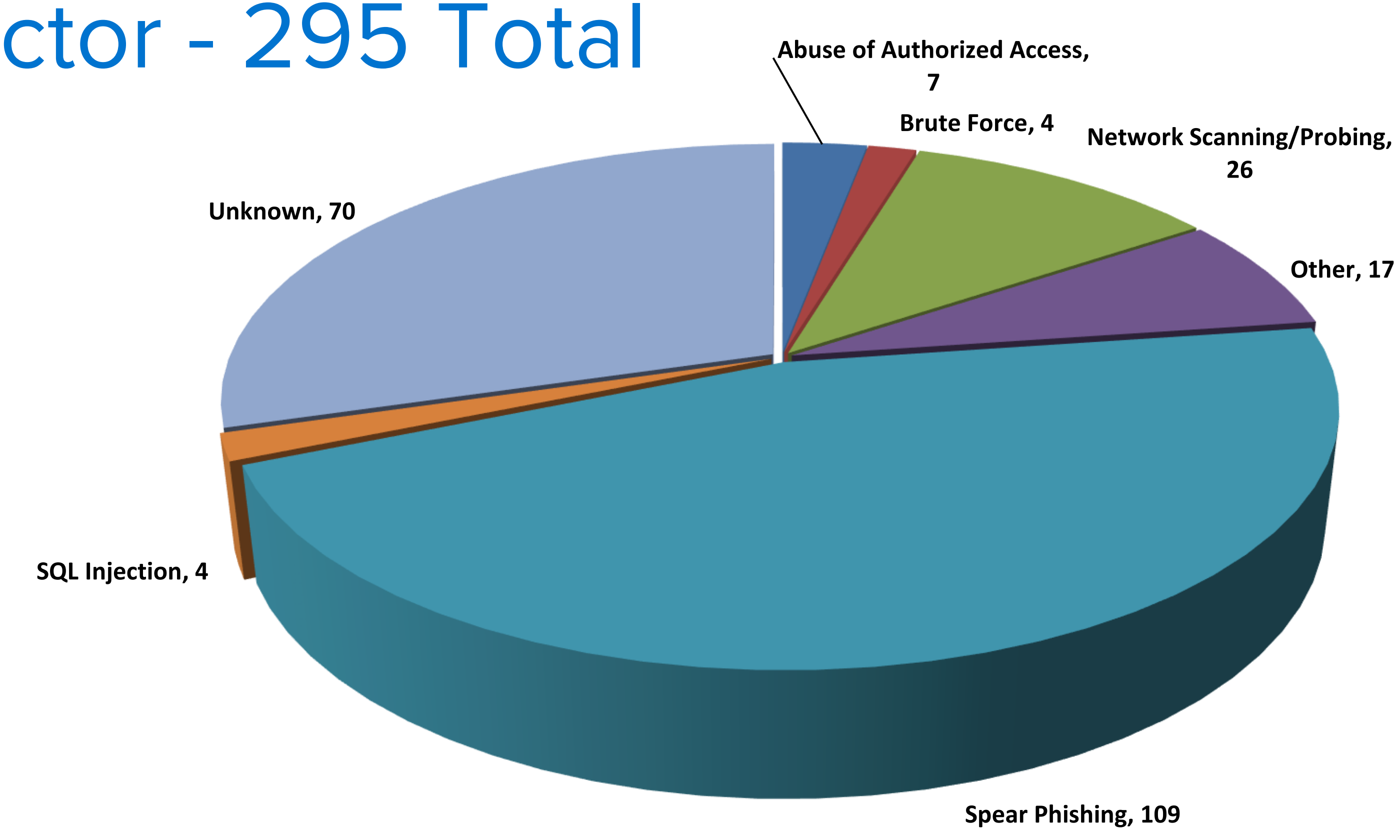
# ICS Incidents FY2015

97 Critical Manufacturing Incidents = 33%

46 Energy Incidents = 16%



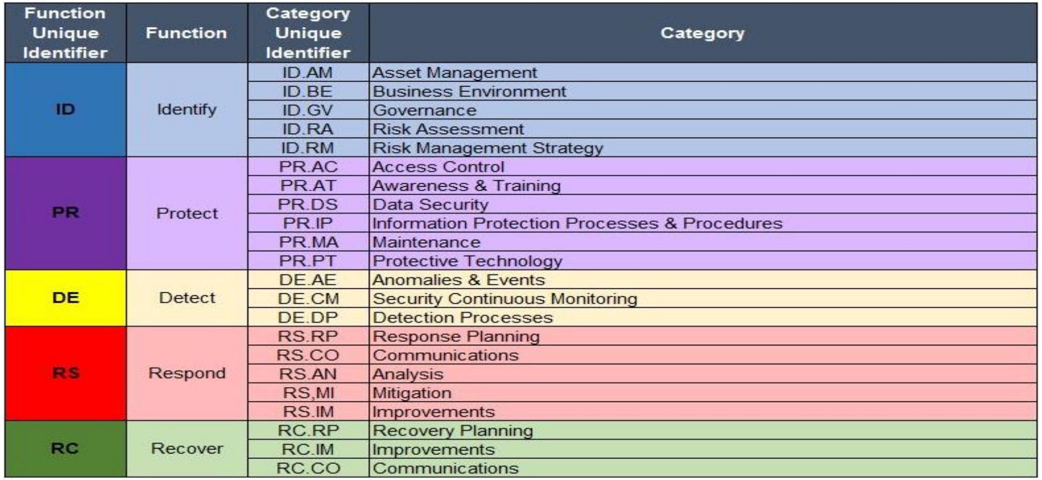
# Fiscal Year 2015 Attempted Infection Vector - 295 Total



UNCLASSIFIED

# Framework for Improving Critical Infrastructure Cybersecurity

- Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in February 2013
- Voluntary framework for reducing cyber risks to critical infrastructure
- Collaboration between industry and government to promote the protection of critical infrastructure
- Prioritized, flexible, repeatable, and cost-effective approach helps manage cyber risks

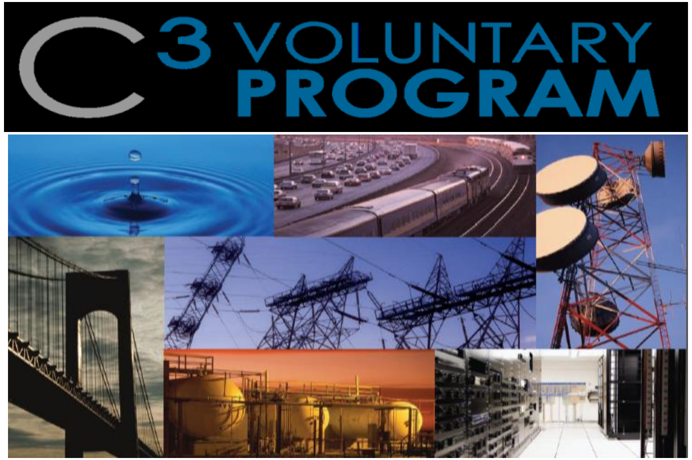


| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| PR | Protect | PR.AC | Access Control |
| | | PR.AT | Awareness & Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes & Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| DE | Detect | DE.AE | Anomalies & Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS,MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

# Critical Infrastructure Cyber Community ($C^3$) Voluntary Program

**Focus areas:**

- Support increasing CI cyber resilience
- Increase awareness of use of the framework
- Encourage orgs to manage cyber as part of hazards approach to enterprise risk management



# National Infrastructure Coordinating Center (NICC)

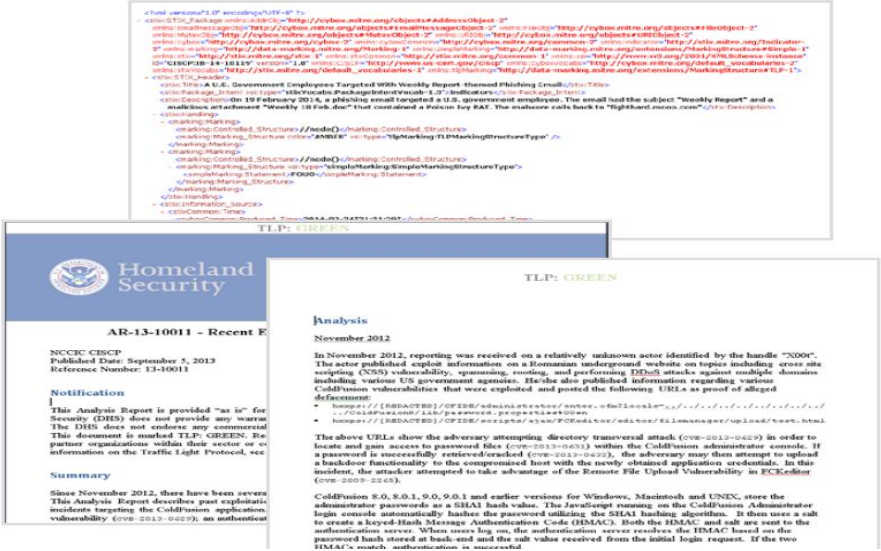
**Focus areas:**

- Situational Awareness
- Information Sharing and Collaboration Processing and posting Suspicious Activity Reports (SAR)
- Assessment and Analysis
- Decision Support
- Future Operations

# Cyber Information Sharing and Collaboration Program (CISCP)

**Focus areas:**

- Indicator Bulletins
- Analysis Reports
- Priority Alerts
- Recommended Practices



```
<?xml version="1.0" encoding="UTF-8" ?>
- <stix:STIX_Package xmlns:AddrObj="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:EmailMessageObj="http://cybox.mitre.org/objects#EmailMessageObject-2" xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
    xmlns:MutexObj="http://cybox.mitre.org/objects#MutexObject-2" xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2"
    xmlns:cybox="http://cybox.mitre.org/cybox-2" xmlns:cyboxCommon="http://cybox.mitre.org/common-2" xmlns:indicator="http://stix.mitre.org/Indicator-
    2" xmlns:marking="http://data-marking.mitre.org/Marking-1" xmlns:simpleMarking="http://data-marking.mitre.org/extensions/MarkingStructure#Simple-1"
    xmlns:stix="http://stix.mitre.org/stix-1" xmlns:stixCommon="http://stix.mitre.org/common-1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    id="CISCP:IB-14-10119" version="1.0" xmlns:CISCP="http://www.us-cert.gov/ciscp" xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1" xmlns:tlpMarking="http://data-marking.mitre.org/extensions/MarkingStructure#TLP-1">
  - <stix:STIX_Header>
      <stix:Title>A U.S. Government Employees Targeted With Weekly Report-themed Phishing Email</stix:Title>
      <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators</stix:Package_Intent>
      <stix:Description>On 19 February 2014, a phishing email targeted a U.S. government employee. The email had the subject "Weekly Report" and a
        malicious attachment "Weekly 18 Feb.doc" that contained a Poison Ivy RAT. The malware calls back to "fighthard.mooo.com"</stix:Description>
    - <stix:Handling>
      - <marking:Marking>
          <marking:Controlled_Structure>//node()</marking:Controlled_Structure>
          <marking:Marking_Structure color="AMBER" xsi:type="tlpMarking:TLPMarkingStructureType" />
        </marking:Marking>
      - <marking:Marking>
          <marking:Controlled_Structure>//node()</marking:Controlled_Structure>
        - <marking:Marking_Structure xsi:type="simpleMarking:SimpleMarkingStructureType">
            <simpleMarking:Statement>FOUO</simpleMarking:Statement>
          </marking:Marking_Structure>
        </marking:Marking>
      </stix:Handling>
    - <stix:Information_Source>
      - <stixCommon:Time>
          <cyboxCommon:Produced_Time>2014-02-24T21:21:29Z</cyboxCommon:Produced_Time>
```

TLP: GREEN

Homeland Security

**AR-13-10011 - Recent E**

NCCIC CISCP
Published Date: September 5, 2013
Reference Number: 13-10011

**Notification**

This Analysis Report is provided "as is" for
Security (DHS) does not provide any warra
The DHS does not endorse any commercial
This document is marked TLP: GREEN. Re
partner organizations within their sector or c
information on the Traffic Light Protocol, see

**Summary**

Since November 2012, there have been severa
This Analysis Report describes past exploitatio
incidents targeting the ColdFusion application
vulnerability (CVE-2013-0629); an authenticat

TLP: GREEN

**Analysis**

November 2012

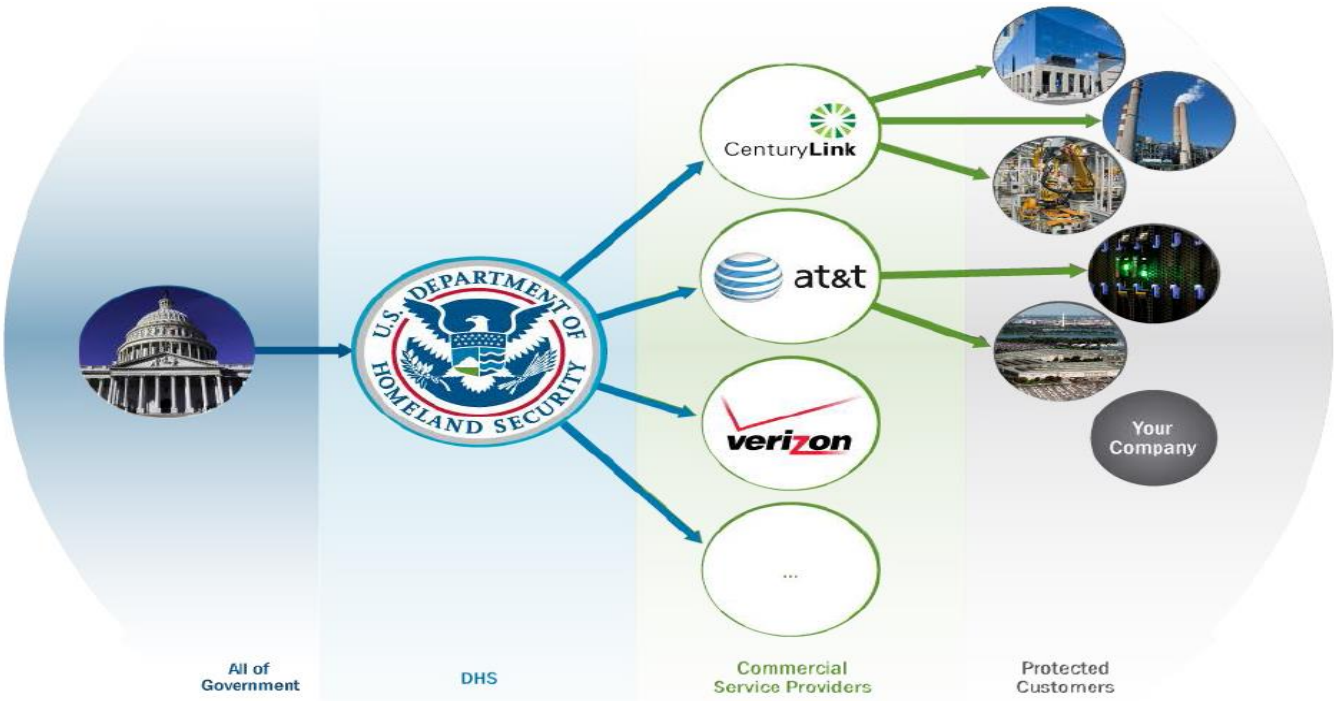
In November 2012, reporting was received on a relatively unknown actor identified by the handle "X00t". The actor published exploit information on a Romanian underground website on topics including cross site scripting (XSS) vulnerability, spamming, rooting, and performing DDoS attacks against multiple domains including various US government agencies. He/she also published information regarding various ColdFusion vulnerabilities that were exploited and posted the following URLs as proof of alleged defacement:

- hxxps://[REDACTED]/CFIDE/administrator/enter.cfm?locale=../../../../../../../../../../ColdFusion8/lib/password.properties%00en
- hxxps://[REDACTED]/CFIDE/scripts/ajax/FCKeditor/editor/filemanager/upload/test.html

The above URLs show the adversary attempting directory transversal attack (CVE-2013-0629) in order to locate and gain access to password files (CVE-2013-0631) within the ColdFusion administrator console. If a password is successfully retrieved/cracked (CVE-2013-0632), the adversary may then attempt to upload a backdoor functionality to the compromised host with the newly obtained application credentials. In this incident, the attacker attempted to take advantage of the Remote File Upload Vulnerability in FCKeditor (CVE-2009-2265).

ColdFusion 8.0, 8.0.1, 9.0, 9.0.1 and earlier versions for Windows, Macintosh and UNIX, store the administrator passwords as a SHA1 hash value. The JavaScript running on the ColdFusion Administrator login console automatically hashes the password utilizing the SHA1 hashing algorithm. It then uses a salt to create a keyed-Hash Message Authentication Code (HMAC). Both the HMAC and salt are sent to the authentication server. When users log on, the authentication server resolves the HMAC based on the password hash stored at back-end and the salt value received from the initial login request. If the two HMACs match, authentication is successful.

# Enhanced Cybersecurity Services (ECS)



UNCLASSIFIED

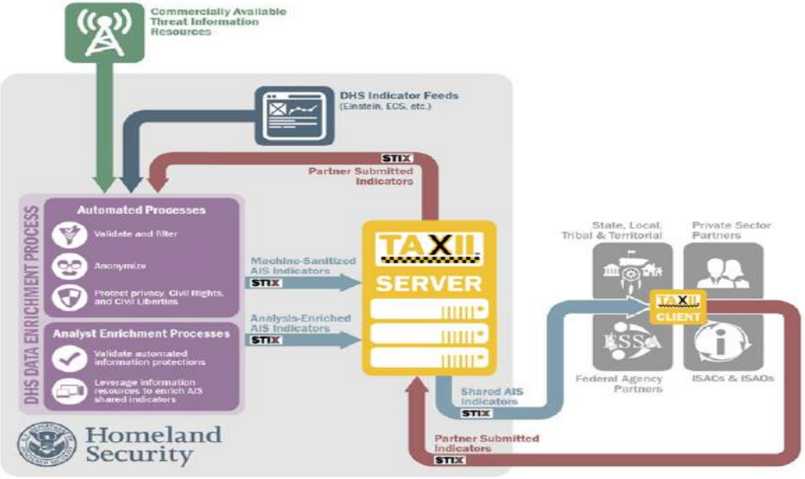
# Automated Information Sharing: STIX/TAXII/CybOX

**TAXII™**, the Trusted Automated eXchange of Indicator Information

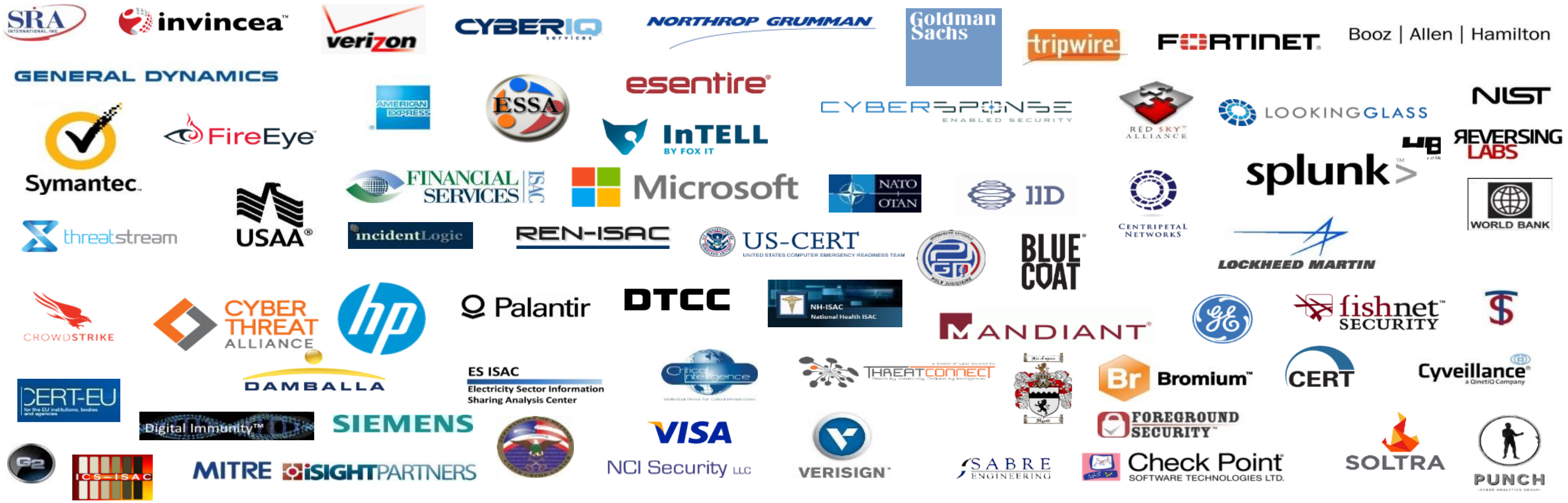
**STIX™**, the Structured Threat Information eXpression

Phases:

- Disseminate computer-readable cyber threat indicators
- Receive, filter, and analyze
- Automate receipt, retention, use, and sharing
- Implement a shared services capability


Commercially Available Threat Information Resources
DHS Indicator Feeds (Einstein, ECS, etc.)
STIX
Partner Submitted Indicators
DHS DATA ENRICHMENT PROCESS
Automated Processes
Validate and filter
Anonymize
Protect privacy, Civil Rights, and Civil Liberties
Analyst Enrichment Processes
Validate automated information protections
Leverage information resources to enrich AIS shared indicators
Machine-Sanitized AIS Indicators
STIX
Analysis-Enriched AIS Indicators
STIX
TAXII
SERVER
Shared AIS Indicators
STIX
Partner Submitted Indicators
STIX
State, Local, Tribal & Territorial
Private Sector Partners
TAXII
CLIENT
Federal Agency Partners
ISACs & ISAOs
Homeland Security

# Automated Information Sharing: STIX/TAXII

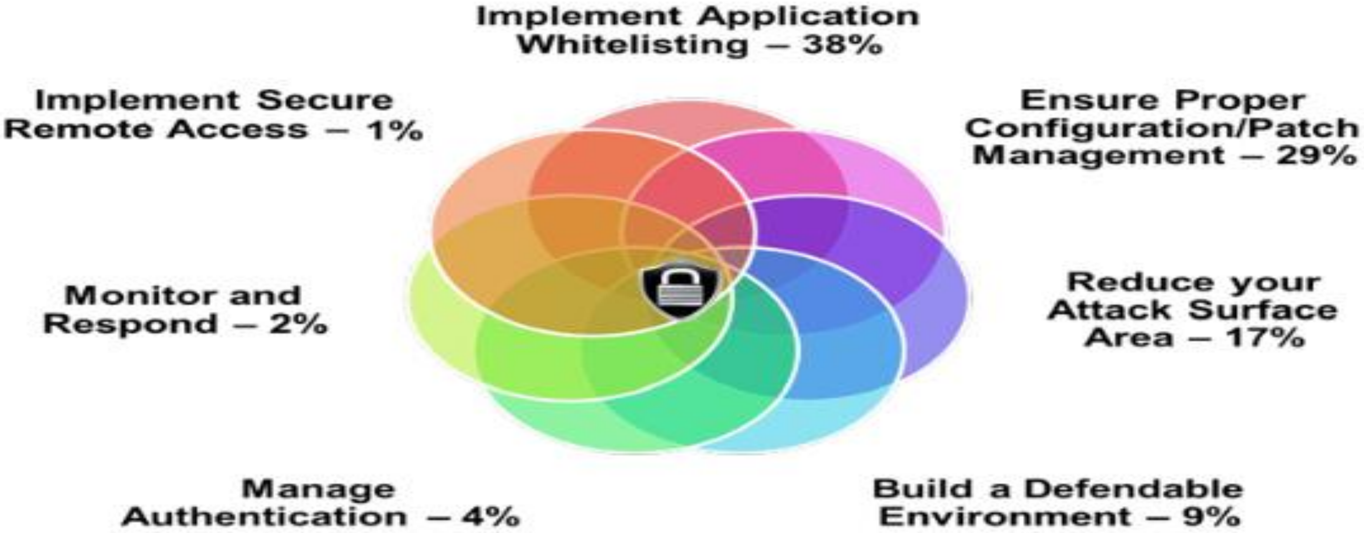


# Information Sharing & Analysis Centers (ISACs)
# Information Sharing & Analysis Org(ISAOs)

NCC
AVIATION ISAC
IT ISAC
A DECADE OF ENABLING RISK MANAGEMENT THROUGH COLLABORATION
ONG-ISAC
ST-ISAC
SC ISAC
HEALTH ISAC
REN-ISAC
APTA
EMR-ISAC
MARITIME ISAC
MARITIME SECURITY COUNCIL
MARITIME INFORMATION SHARING & ANALYSIS CENTER
NEI
Real Estate ISAC Information Sharing and Analysis Center
ES-ISAC
FINANCIAL SERVICES ISAC
WaterISAC
DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER
MULTI-STATE ISAC

DHS INFORMATION SHARING PROGRAMS
ISAO
ISAC
ISAC
ISAO
ISAO
ISAC
U.S. DEPARTMENT OF HOMELAND SECURITY
DHS INFORMATION SHARING PROGRAMS

# Seven Steps to Effectively Defend Industrial Control Systems



Implement Application Whitelisting – 38%

Ensure Proper Configuration/Patch Management – 29%

Reduce your Attack Surface Area – 17%

Build a Defendable Environment – 9%

Manage Authentication – 4%

Monitor and Respond – 2%

Implement Secure Remote Access – 1%

# Contact DHS ICS-CERT

ICS CERT encourages you to report suspicious activity and vulnerabilities affecting critical infrastructure control systems

To report control systems cyber incidents and vulnerabilities contact ICS-CERT:

- Toll Free: 1-877-776-7585
- International Callers: 1-208-526-0900
- Ics-cert@hq.dhs.gov

For industrial control systems security information and incident reporting:

- http://ics-cert.us-cert.gov

Homeland Security

# Contact Information

Darryl E. Peek II

Darryl.peek@hq.dhs.gov

DHS/OCIO/OCTO