2017 New York State Cybersecurity Conference

Cybersecurity Policy Overview

June 7, 2017

Robert H. Mayer
USTelecom , Vice-President - Industry and State Affairs
Chair, Communications Sector Coordinating Council (CSCC)

Content

- National Cybersecurity Ecosystem
  - Departments and Agencies
  - Roles and Responsibilities

- Cybersecurity Initiatives Across Federal Landscape

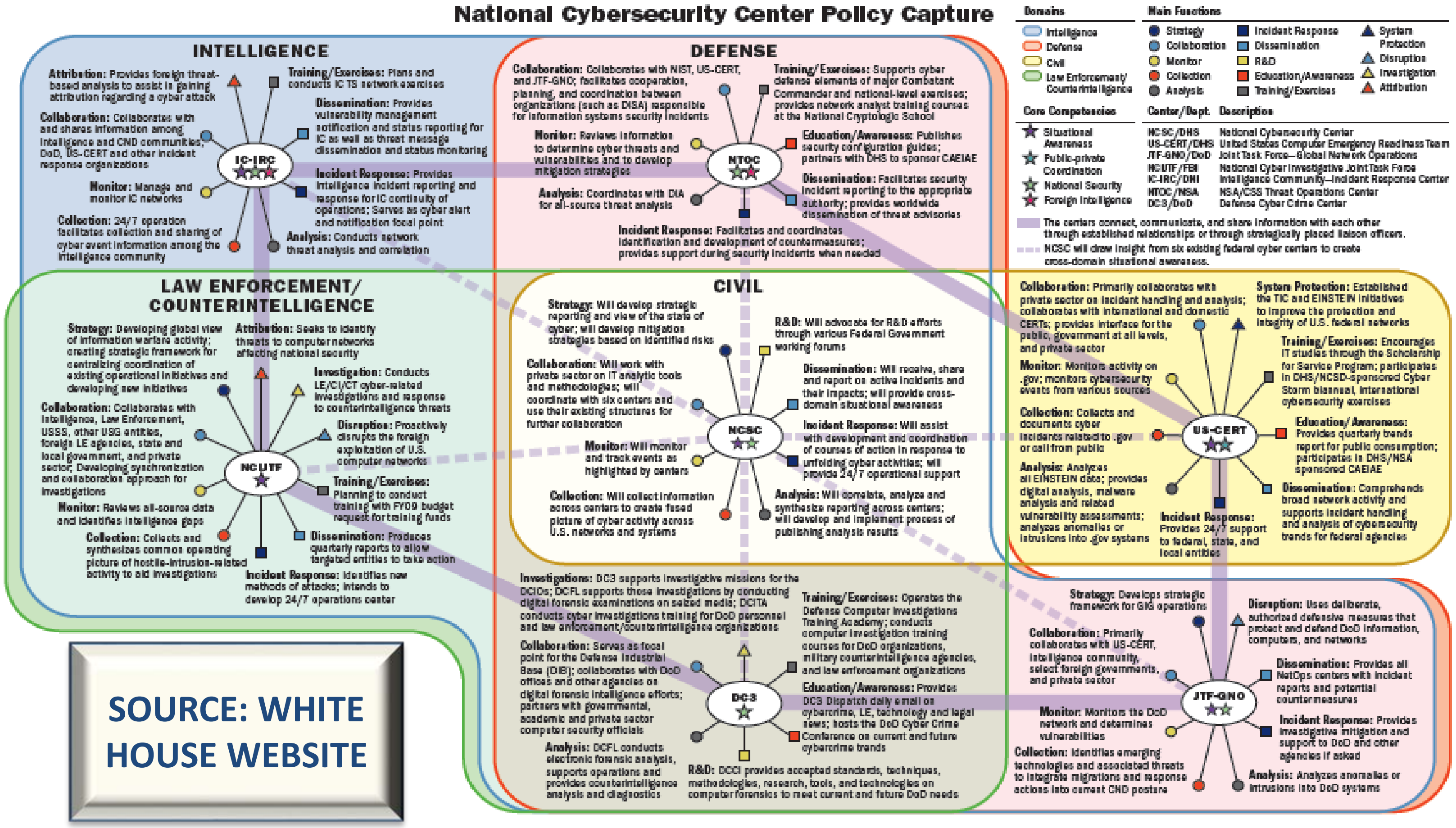
- Critical Policy Issues & Venues
  - Information Sharing
  - Incident Response
  - Risk Management
  - Internet of Things

- Recent Cybersecurity Executive Order

- Discussion

Multi-layered Authority And Engagement

Cyber capabilities in the US are challenging to map in a comprehensive manner. The tendency to layer initiatives and agencies makes navigating the different components difficult. **Rand Europe – September 2015**



National Cybersecurity Center Policy Capture

INTELLIGENCE

IC-IRC

Attribution: Provides foreign threat-based analysis to assist in gaining attribution regarding a cyber attack

Training/Exercises: Plans and conducts IC TS network exercises

Collaboration: Collaborates with and shares information among Intelligence and CND communities, DoD, US-CERT and other incident response organizations

Dissemination: Provides vulnerability management notification and status reporting for IC as well as threat message dissemination and status monitoring

Monitor: Manage and monitor IC networks

Incident Response: Provides Intelligence incident reporting and response for IC continuity of operations; Serves as cyber alert and notification focal point

Collection: 24/7 operation facilitates collection and sharing of cyber event information among the intelligence community

Analysis: Conducts network threat analysis and correlation

DEFENSE

NTOC

Collaboration: Collaborates with NIST, US-CERT, and JTF-GNO; facilitates cooperation, planning, and coordination between organizations (such as DISA) responsible for information systems security incidents

Training/Exercises: Supports cyber defense elements of major Combatant Commander and national-level exercises; provides network analyst training courses at the National Cryptologic School

Monitor: Reviews information to determine cyber threats and vulnerabilities and to develop mitigation strategies

Education/Awareness: Publishes security configuration guides; partners with DHS to sponsor CAEIAE

Analysis: Coordinates with DIA for all-source threat analysis

Dissemination: Facilitates security incident reporting to the appropriate authority; provides worldwide dissemination of threat advisories

Incident Response: Facilitates and coordinates identification and development of countermeasures; provides support during security incidents when needed

LAW ENFORCEMENT/ COUNTERINTELLIGENCE

NCIJTF

Strategy: Developing global view of information warfare activity; creating strategic framework for centralizing coordination of existing operational initiatives and developing new initiatives

Attribution: Seeks to identify threats to computer networks affecting national security

Investigation: Conducts LE/CI/CT cyber-related investigations and response to counterintelligence threats

Collaboration: Collaborates with Intelligence, Law Enforcement, USSS, other USG entities, foreign LE agencies, state and local government, and private sector; Developing synchronization and collaboration approach for investigations

Disruption: Proactively disrupts the foreign exploitation of U.S. computer networks

Training/Exercises: Planning to conduct training with FY09 budget request for training funds

Monitor: Reviews all-source data and identifies intelligence gaps

Collection: Collects and synthesizes common operating picture of hostile-intrusion-related activity to aid investigations

Dissemination: Produces quarterly reports to allow targeted entities to take action

Incident Response: Identifies new methods of attacks; intends to develop 24/7 operations center

CIVIL

NCSC

Strategy: Will develop strategic reporting and view of the state of cyber; will develop mitigation strategies based on identified risks

R&D: Will advocate for R&D efforts through various Federal Government working forums

Collaboration: Will work with private sector on IT analytic tools and methodologies; will coordinate with six centers and use their existing structures for further collaboration

Dissemination: Will receive, share and report on active incidents and their impacts; will provide cross-domain situational awareness

Monitor: Will monitor and track events as highlighted by centers

Incident Response: Will assist with development and coordination of courses of action in response to unfolding cyber activities; will provide 24/7 operational support

Collection: Will collect information across centers to create fused picture of cyber activity across U.S. networks and systems

Analysis: Will correlate, analyze and synthesize reporting across centers; will develop and implement process of publishing analysis results

DC3

Investigations: DC3 supports investigative missions for the DCIOs; DCFL supports those investigations by conducting digital forensic examinations on seized media; DCITA conducts cyber investigations training for DoD personnel and law enforcement/counterintelligence organizations

Training/Exercises: Operates the Defense Computer Investigations Training Academy; conducts computer investigation training courses for DoD organizations, military counterintelligence agencies, and law enforcement organizations

Collaboration: Serves as focal point for the Defense Industrial Base (DIB); collaborates with DoD offices and other agencies on digital forensic intelligence efforts; partners with governmental, academic and private sector computer security officials

Education/Awareness: Provides DC3 Dispatch daily email on cybercrime, LE, technology and legal news; hosts the DoD Cyber Crime Conference on current and future cybercrime trends

Analysis: DCFL conducts electronic forensic analysis, supports operations and provides counterintelligence analysis and diagnostics

R&D: DCCI provides accepted standards, techniques, methodologies, research, tools, and technologies on computer forensics to meet current and future DoD needs

US-CERT

Collaboration: Primarily collaborates with private sector on incident handling and analysis; collaborates with international and domestic CERTs; provides interface for the public, government at all levels, and private sector

System Protection: Established the TIC and EINSTEIN initiatives to improve the protection and integrity of U.S. federal networks

Training/Exercises: Encourages IT studies through the Scholarship for Service Program; participates in DHS/NCSD-sponsored Cyber Storm biannual, international cybersecurity exercises

Monitor: Monitors activity on .gov; monitors cybersecurity events from various sources

Collection: Collects and documents cyber incidents related to .gov or call from public

Education/Awareness: Provides quarterly trends report for public consumption; participates in DHS/NSA sponsored CAEIAE

Analysis: Analyzes all EINSTEIN data; provides digital analysis, malware analysis and related vulnerability assessments; analyzes anomalies or intrusions into .gov systems

Incident Response: Provides 24/7 support to federal, state, and local entities

Dissemination: Comprehends broad network activity and supports incident handling and analysis of cybersecurity trends for federal agencies

JTF-GNO

Strategy: Develops strategic framework for GIG operations

Disruption: Uses deliberate, authorized defensive measures that protect and defend DoD information, computers, and networks

Collaboration: Primarily collaborates with US-CERT, intelligence community, select foreign governments, and private sector

Dissemination: Provides all NetOps centers with incident reports and potential countermeasures

Monitor: Monitors the DoD network and determines vulnerabilities

Incident Response: Provides investigative mitigation and support to DoD and other agencies if asked

Collection: Identifies emerging technologies and associated threats to integrate migrations and response actions into current CND posture

Analysis: Analyzes anomalies or intrusions into DoD systems

Domains

- Intelligence
- Defense
- Civil
- Law Enforcement/ Counterintelligence

Main Functions

- ● Strategy
- ● Collaboration
- ● Monitor
- ● Collection
- ● Analysis
- ■ Incident Response
- ■ Dissemination
- ■ R&D
- ■ Education/Awareness
- ■ Training/Exercises
- ▲ System Protection
- ▲ Disruption
- ▲ Investigation
- ▲ Attribution

Core Competencies

- ★ Situational Awareness
- ★ Public-private Coordination
- ★ National Security
- ★ Foreign Intelligence

Center/Dept.	Description
NCSC/DHS	National Cybersecurity Center
US-CERT/DHS	United States Computer Emergency Readiness Team
JTF-GNO/DoD	Joint Task Force—Global Network Operations
NCIJTF/FBI	National Cyber Investigative Joint Task Force
IC-IRC/DNI	Intelligence Community—Incident Response Center
NTOC/NSA	NSA/CSS Threat Operations Center
DC3/DoD	Defense Cyber Crime Center

The centers connect, communicate, and share information with each other through established relationships or through strategically placed liaison officers.

NCSC will draw insight from six existing federal cyber centers to create cross-domain situational awareness.

SOURCE: WHITE HOUSE WEBSITE

UNCLASSIFIED

AGREED
March 5, 2013

U.S. Federal Cybersecurity Operations Team

National Roles and Responsibilities*

US Government Departments and Agencies

DOJ/FBI

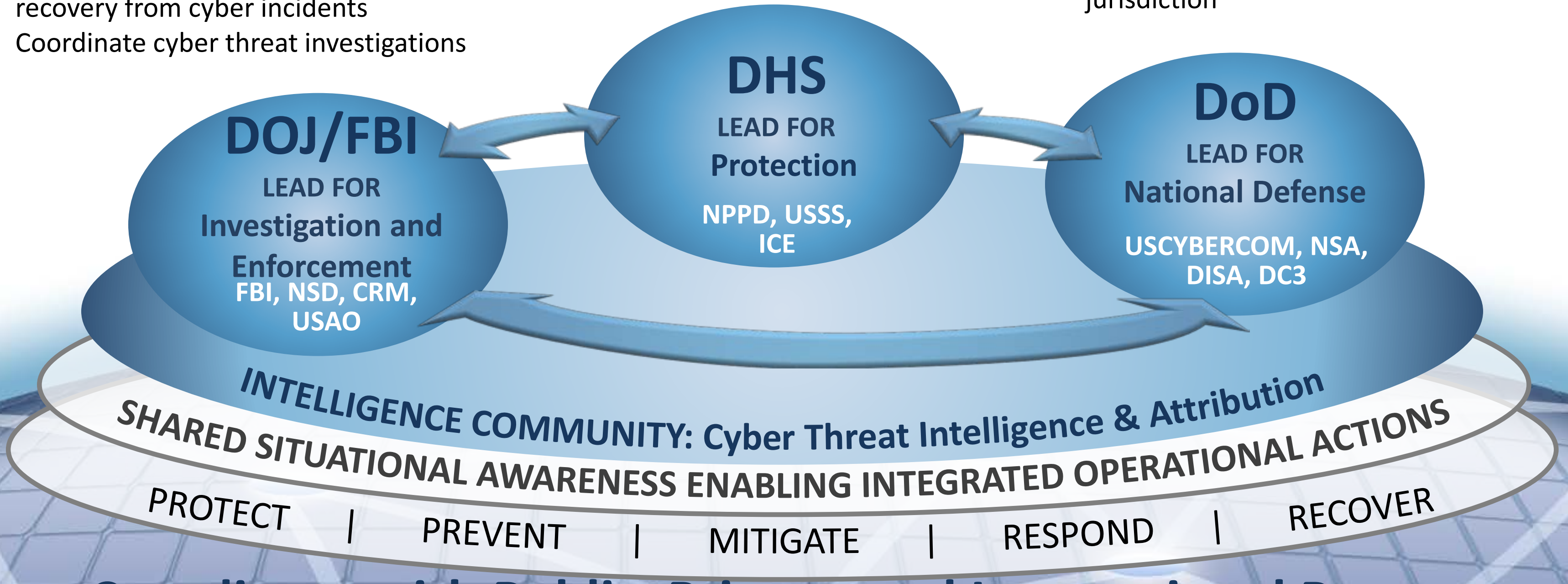
- Investigate, attribute, disrupt and prosecute cyber crimes
- Lead domestic national security operations
- Conduct domestic collection, analysis, and dissemination of cyber threat intelligence
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Coordinate cyber threat investigations

DHS

- Coordinate the national protection, prevention, mitigation of, and recovery from cyber incidents
- Disseminate domestic cyber threat and vulnerability analysis
- Protect critical infrastructure
- Secure federal civilian systems
- Investigate cyber crimes under DHS's jurisdiction

DoD

- Defend the nation from attack
- Gather foreign cyber threat intelligence and determine attribution
- Secure national security and military systems
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Investigate cyber crimes under military jurisdiction



DOJ/FBI
LEAD FOR
Investigation and Enforcement
FBI, NSD, CRM, USAO

DHS
LEAD FOR
Protection
NPPD, USSS, ICE

DoD
LEAD FOR
National Defense
USCYBERCOM, NSA, DISA, DC3

INTELLIGENCE COMMUNITY: Cyber Threat Intelligence & Attribution

SHARED SITUATIONAL AWARENESS ENABLING INTEGRATED OPERATIONAL ACTIONS

PROTECT | PREVENT | MITIGATE | RESPOND | RECOVER

Global Cyberspace

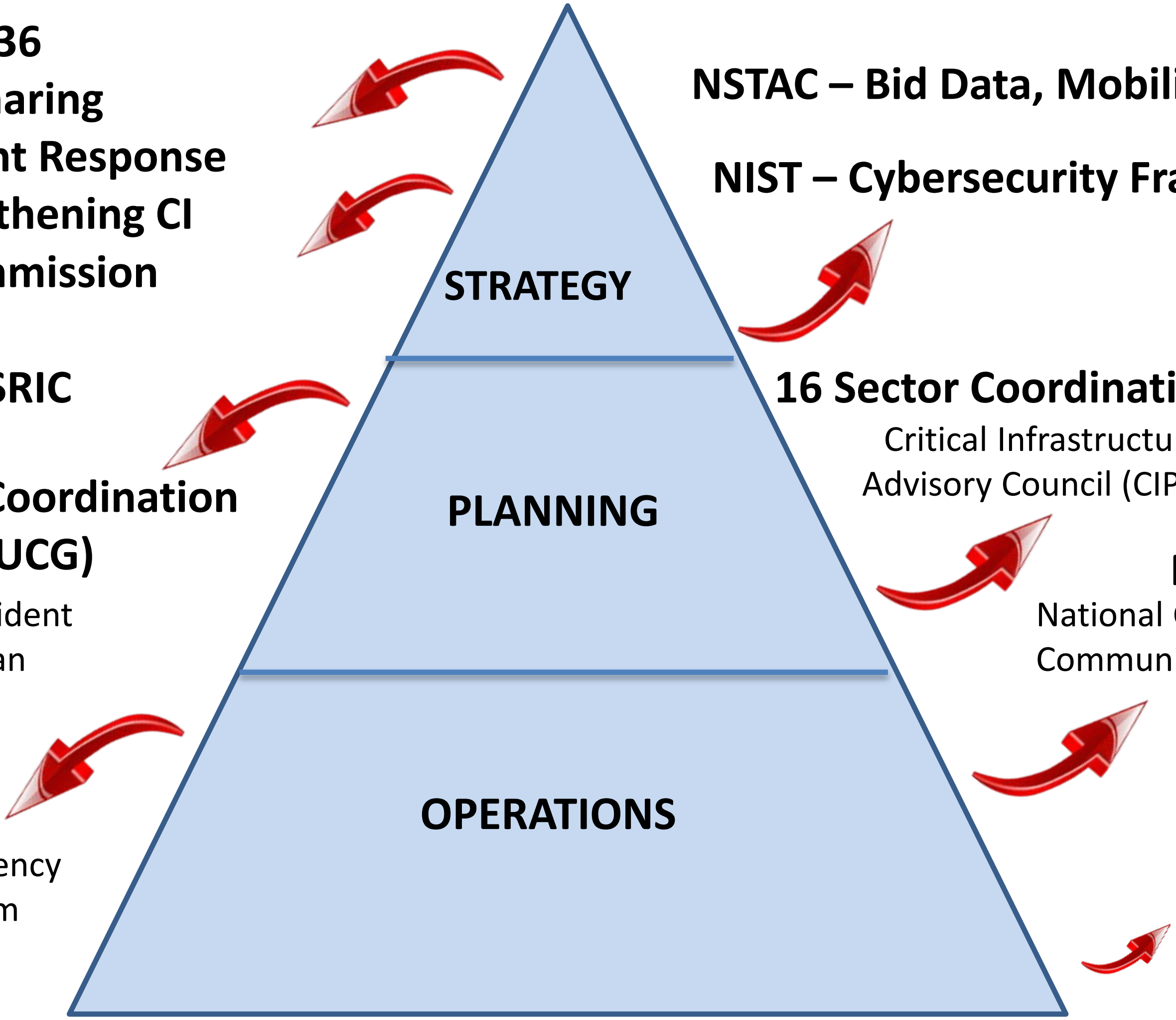
Coordinate with Public, Private, and International Partners

** Note: Nothing in this chart alters existing DOJ, DHS, and DoD roles, responsibilities, or authorities*

UNCLASSIFIED

Partnership Construct

The Public-Private Partnership Operates on Multiple Levels



White House EOP

EO13636

Info Sharing

Incident Response

Strengthening CI

CNAP Commission

FCC CSRIC

Cyber Unified Coordination Group (UCG)

National Cyber Incident Response Plan

USCERT

US Computer Emergency Readiness Team

NSTAC – Bid Data, Mobilization, Quantum

NIST – Cybersecurity Framework 1.1

16 Sector Coordinating Councils

Critical Infrastructure Partnership Advisory Council (CIPAC) (PCIS)

NCICC

National Cybersecurity and Communications Integrations Center

NCC-Comms

ISAC

CyberStorm VI

USTELECOM
THE BROADBAND ASSOCIATION

Current Cyber Initiatives

WH

- Executive Order
- Presidential Cybersecurity Commission (Published in December 2016)
- NSTAC Emerging Technology Strategic Vision (ETSV) Report

Congress

- Oversight on Implementation of CISA (CISA – Passed 12/15) - Focus on implementation
- Potential DHS Re organization bill
- Ongoing inquiries on IoT Security Issues

FCC

- FCC 5G NOI
- FCC Privacy
- FCC Tech Transitions NPRM
- FCC Spectrum Frontiers NPRM
- CSRIC V – WG 5 Information Sharing, WG 6 Supply Chain, WG 7 Workforce, WG 9 Wi-Fi Security, WG10 SS7
- FCC TAC – IoT, SDN/NFV, Smart Phone Security Tracker
- FCC Policy Statement/ Company specific meetings
- CSRIC VI (about to commence)

Commerce/NIST/NTIA

- IoT RFC Comments
- NIST RFI Framework 1.1
- NTIA Internet Security Taskforce - Upgradeability
- OMB/Commerce/EOP Baldridge Award Program
- NIST privacy engineering (Published in January)
- BIS Export Controls (Wassanaar Agreement)
- NIST Mobile Threat Catalog (NISTIR-8144)

DHS

- National Cybersecurity Incident Response Plan (NCIRP)
- DHS IoT Principles
- DHS ISAO Standards Development
- DHS Automated Indicator Sharing Portal (AIS)/CISA Implementation
- DHS Organizational Structure Changes
- DHS CIDAR Initiative (Cyber Incident Database)
- DHS PCII RFC (Updating PCII office process)

States

- NARUC
- State Regulatory Proceedings - Connecticut/ Illinois/ Missouri/ New Jersey etc.
- New York AG Proposal for Financial Institutions
- NAG/NCSL Cybersecurity Initiatives

Other

- Cybersecurity Forum for Independent and Executive Branch Regulators
- FTC/CFPB PCI Auditing Review
- FTC Enforcement Actions
- NHTSA Connected Car/GAO Report
- FTC Ransomware Workshop 9/7

CSCC
COMMUNICATIONS SECTOR COORDINATING COUNCIL

Key Policy Initiatives

Information Sharing

Initiatives designed in response to a perceived and real need to create more formal and structured info sharing venues where actionable and timely cyber threat indicators are shared between private to private, private to government and government to private entities.

Internet of Things (IoT)

Initiatives designed in response to the exponential growth of Internet-connected devices and the relatively poor security capabilities that are part of the design phase. The recent Dyn attack put a spotlight on the risk that IoT poses to a broad set of infrastructure providers.

Risk Management Frameworks

Most notably the NIST Cybersecurity Framework (CSF) that embodied a flexible and “no one-size-fits-all” construct for enterprises to manage risk in accordance with their unique risk profile and tolerance. The NIST CSF has been widely embraced by industry because it is viewed as an important alternative to counter-productive prescriptive regimes.

Incident Response

Mechanisms for individual enterprises to respond to a cyber crisis and for government and industry to coordinate efforts required to mitigate and recover from more consequential attacks

Key Initiatives and Venues

	White House	DoC	DHS	FTC	FCC	DoD	The Hill
Information Sharing	✓	✓	✓		✓	✓	✓
Internet of Things	✓	✓	✓	✓		✓	✓
Risk Management	✓	✓	✓	✓	✓	✓	✓
Incident Response	✓		✓		✓	✓	✓

Key Provisions of Latest Cyber Executive Order

Federal Networks

The President will hold heads of **executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises.** In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to **manage cybersecurity risk as an executive branch enterprise.**

Effective immediately, **each agency head shall use The Framework** for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk.

establish a regular process for reassessing and, if appropriate, reissuing the determination, and addressing future, **recurring unmet budgetary needs** necessary to manage risk to the executive branch enterprise

Key Provisions (continued)

Critical Infrastructure

It is the policy of the executive branch to use its authorities and capabilities **to support the cybersecurity risk management efforts of the owners and operators** of the Nation's critical infrastructure

identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities identified **pursuant to section 9** of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), to be at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security (section 9 entities

engage section 9 entities and solicit input as appropriate to evaluate whether and how the authorities and capabilities…might be employed to support cybersecurity risk management efforts and any obstacles to doing so

Key Provisions (continued)

examine the sufficiency of existing Federal policies and practices to promote appropriate **market transparency of cybersecurity risk management** practices by critical infrastructure entities, with a focus on publicly traded critical infrastructure entities.

lead an open and transparent process to identify and promote action by appropriate stakeholders **to improve the resilience of the internet and communications ecosystem** and to encourage collaboration with the goal of **dramatically reducing** threats perpetrated by automated and distributed attacks (e.g., botnets).

assess:
(i) the potential scope and duration of a prolonged power outage associated with **a significant cyber incident**
(ii) **the readiness** of the United States to **manage the consequences** of such an incident; and
(iii) any **gaps or shortcomings** in assets or capabilities required to **mitigate the consequences** of such an incident.

Key Reports/Resources

COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

DECEMBER 1, 2016

REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY

https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

NIST

CYBERSECURITY FRAMEWORK

https://www.nist.gov/cyberframework

Presidential Executive Order On Strengthening the Cyber-Security of Federal Networks and Critical Infrastructure

THE WHITE HOUSE
WASHINGTON

https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal