

# Cybersecurity Executive Order Impact on Industry and Government



June 3, 2014



17<sup>th</sup> Annual New York State  
Cyber Security Conference

Robert Mayer  
USTelecom Association  
Vice-President Industry & State Affairs

The Evolving Cybersecurity Puzzle

Cyber Threat and Policy Landscape

2013 Cybersecurity Executive Order

NIST Develops the Cybersecurity Framework

DHS Initiates the “C-Cubed” Program

FCC/CSRIC Cyber Risk Management

Discussion

Resources



Links to all referenced initiatives can be located in Resource Section

# An Evolving Puzzle

**REGULATION/  
STANDARD  
OF CARE**

**GOVERNANCE  
&  
OVERSIGHT**

**CRITICAL  
INFRASTRUCTURE**

**REPUTATIONAL  
HARM  
AND  
MARKET RISK**

**SKILLED  
CYBER  
PROS**

**SYSTEMIC  
RISK**

**BUSINESS  
CASE  
(ROI)**

**LIABILITY/  
INSURANCE**

**PRIVACY**

**BYOD**

**ASSET  
MANAGEMENT**

**CLOUD  
COMPUTING**

**MALWARE  
AS A  
SERVICE  
(MaaS)**

**TRUSTED  
IDENTITIES**

**AUDITS  
&  
BENCHMARKING**

**SUPPLY  
CHAIN**

Cyber attacks move to cloud with increased adoption, report shows

**Cyber Threats to Healthcare Systems, Medical Devices Rising**

**Deceptive downloads top threats: Microsoft**

Deceptive downloads faced with malware are the most common cyber security threats, tech giant Microsoft reported on Friday.

Microsoft's 16th Security Intelligence Report (SIR) showed that 95% of 110 countries in the study reported deceptive downloads in the second half of 2013.

Like 4 Facebook Tweet LinkedIn Google+ ShareThis

RELATED STORIES

DoJ close to wrapping up

**Retail Shortfall in Assessing Cyber Threats: Willis**

Silence & inadeq sector

Some retailers in the Fortune 1000 reveals possible cyber liability coverage for some in the retail

**First Heartbleed attack reported; taxpayer da**

Canadian police arrest a man used th

social insurance

**North American grid is vulnerable to cyber attacks**

April 26, 2014 SHANE HARRIS

**The Blue Screen of Death at 30,000 Feet**

**Boston Children's Hospital comes under repeated cyber attacks**



**Top Cyberthreats Exposed by Verizon Report**

By Jennifer LeClaire  
April 22, 2014 11:20AM

**Russian cyber attacks on Ukraine: the Georgia template**

**Russian cyber attacks on Ukraine: the Georgia template**

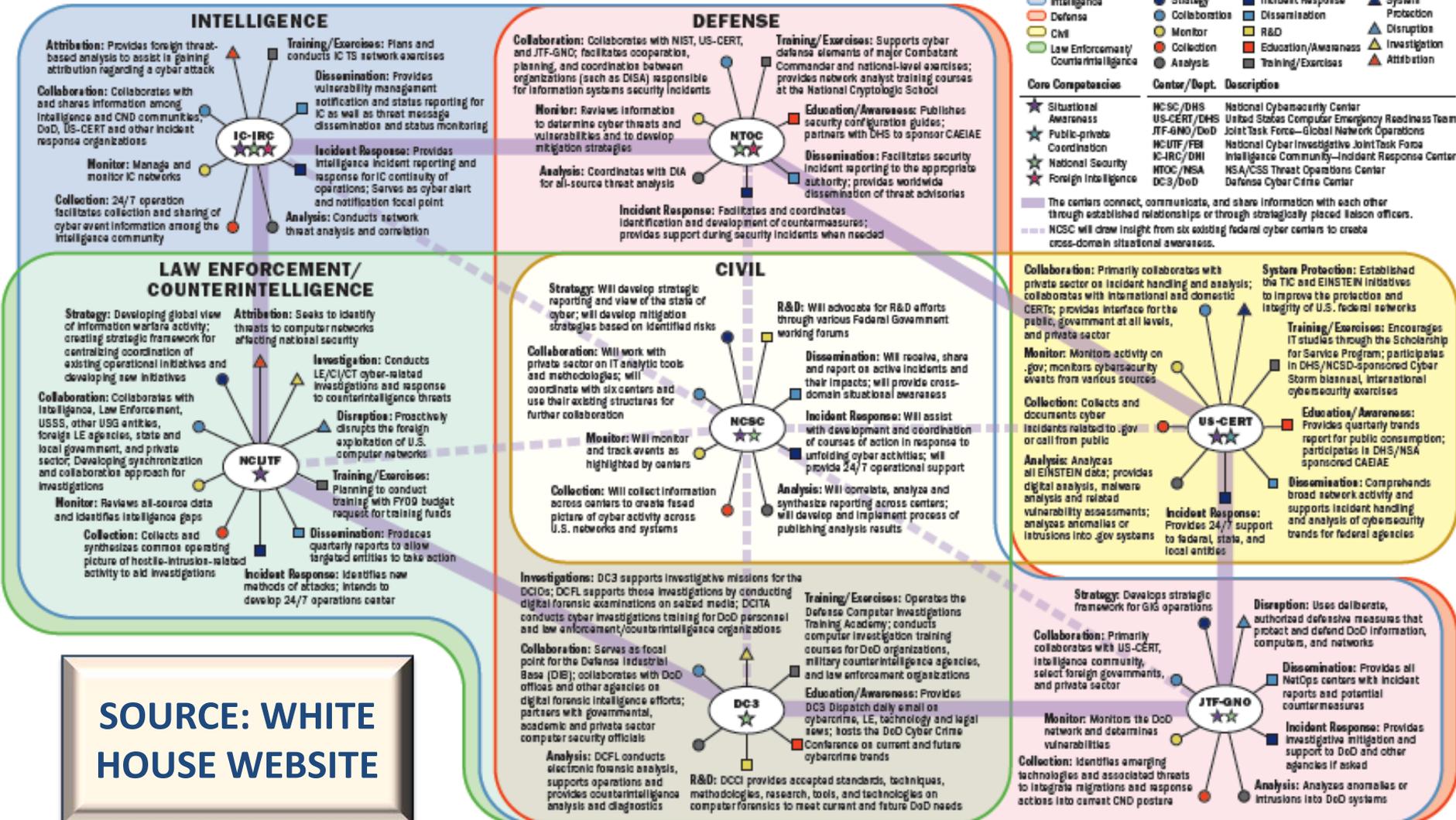
**Target's Data Breach Should Be A Wake Up Call For Energy Companies: No More Excuses On Cyber Threats**

In its 2014 Data Breach Investigations Report, Verizon found that more than 20 percent of a

**Cyber attacks on Lockheed Martin quadruple**

Share this article: Facebook Twitter LinkedIn Google+

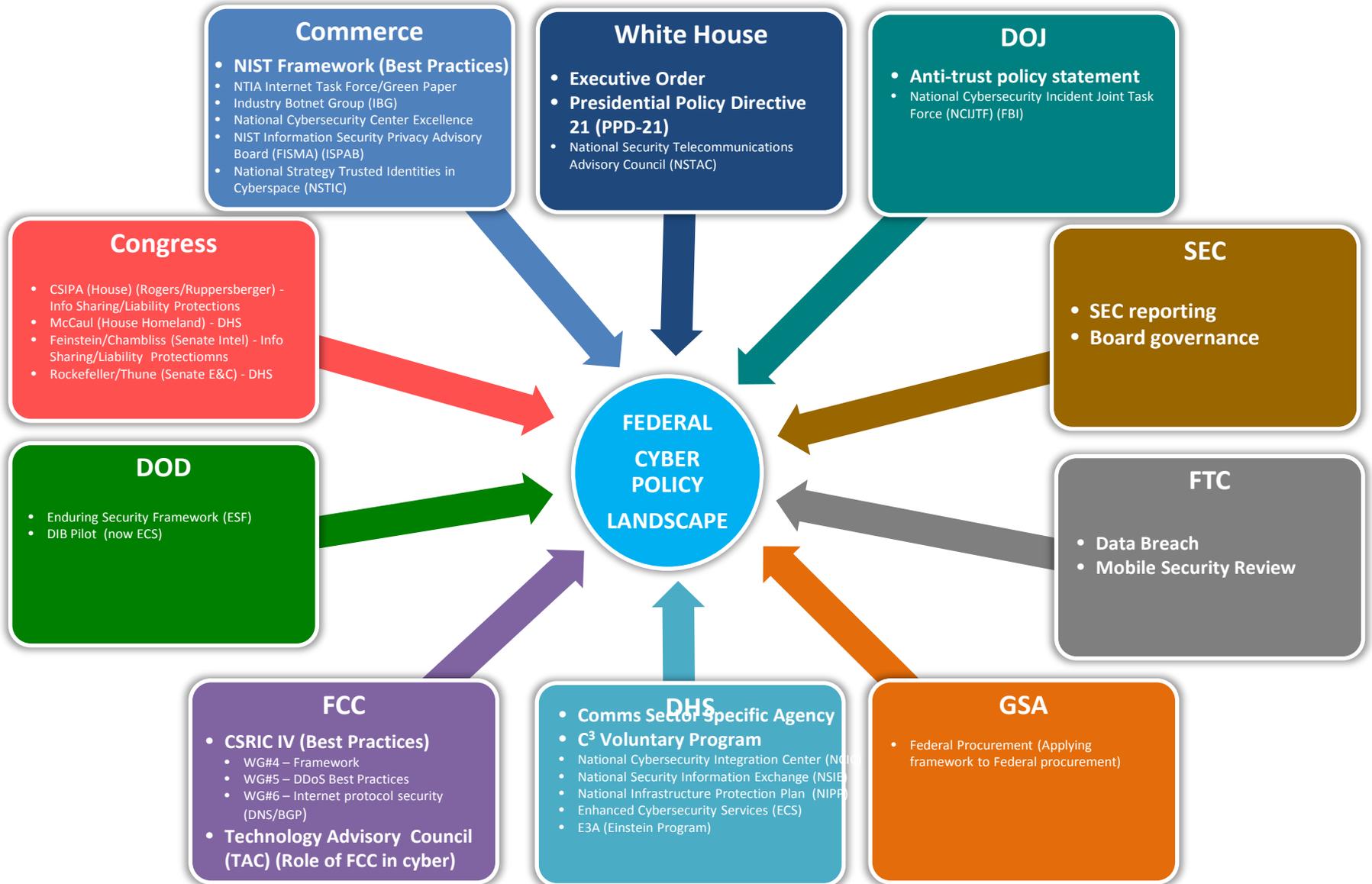
## National Cybersecurity Center Policy Capture



SOURCE: WHITE HOUSE WEBSITE



# Federal Cyber Policy Landscape





# Federal Cyber Policy Landscape

## Commerce

- NIST Framework (Best Practices)
- NTIA Internet Task Force/Green Paper
- Industry Botnet Group (IBG)
- National Cybersecurity Center Excellence
- NIST Information Security Privacy Advisory Board (FISMA) (ISPAB)
- National Strategy Trusted Identities in Cyberspace (NSTIC)

## White House

- Executive Order
- Presidential Policy Directive 21 (PPD-21)
- National Security Telecommunications Advisory Committee (NSTAC)

## DOJ

- Anti-trust policy statement
- National Cybersecurity Incident Joint Task Force (NCIJTF) (FBI)

## DHS

- Comms Sector Specific Agency
- C<sup>3</sup> Voluntary Program
- National Cybersecurity Integration Center (NCIC)
- National Security Information Exchange (NSIE)
- National Infrastructure Protection Plan (NIPP)
- Enhanced Cybersecurity Services (ECS)
- E3A (Einstein Program)

## GSA

- Federal Procurement (Applying framework to Federal procurement)

## FCC

- CSRIC IV (Best Practices)
  - WG#4 – Framework
  - WG#5 – DDoS Best Practices
  - WG#6 – Internet protocol security (DNS/BGP)
- Technology Advisory Council (TAC) (Role of FCC in cyber)

## SEC

- SEC reporting
- Board governance

## FTC

- Data Breach
- Mobile Security Review

## DOD

- Enduring Security Framework (ESF)
- DIB Pilot (now ECS)

Congress

It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. **We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.**



White House  
Executive Order 13636  
February 12, 2013

# Executive Order

## Key Provisions

Sec. 2. Critical Infrastructure. As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Sec. 4. Cybersecurity Information Sharing. (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats.

Sec. 6. Consultative Process. The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure.

Sec. 7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure. (a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework").

Sec. 8. Voluntary Critical Infrastructure Cybersecurity Program. (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the "Program").

Sec. 9. Identification of Critical Infrastructure at Greatest Risk. (a) Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

Sec. 10. Adoption of Framework. (a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks.

## Executive Order Directives

Help owners and operators of critical infrastructure identify, assess, and manage cyber risk

Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach to help owners and operators of critical infrastructure identify, assess, and manage cyber risk

Provide guidance that is technology neutral and enables critical infrastructure sectors to benefit from a competitive market for products and services

Identify security standards and guidelines applicable across sectors of critical infrastructure, while identifying areas that should be addressed through future collaboration with particular sectors and standards-developing organizations

Include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures

Include guidance for measuring the performance of implementing the Framework

## Selected Excerpts From the NIST Cybersecurity Framework

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure.

Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary.

Framework provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today.

Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

## Selected Excerpts From the NIST Cybersecurity Framework

The Framework complements, and does not replace, an organization's risk management process and cybersecurity program.

The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices.

Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.

# Framework Core Structure

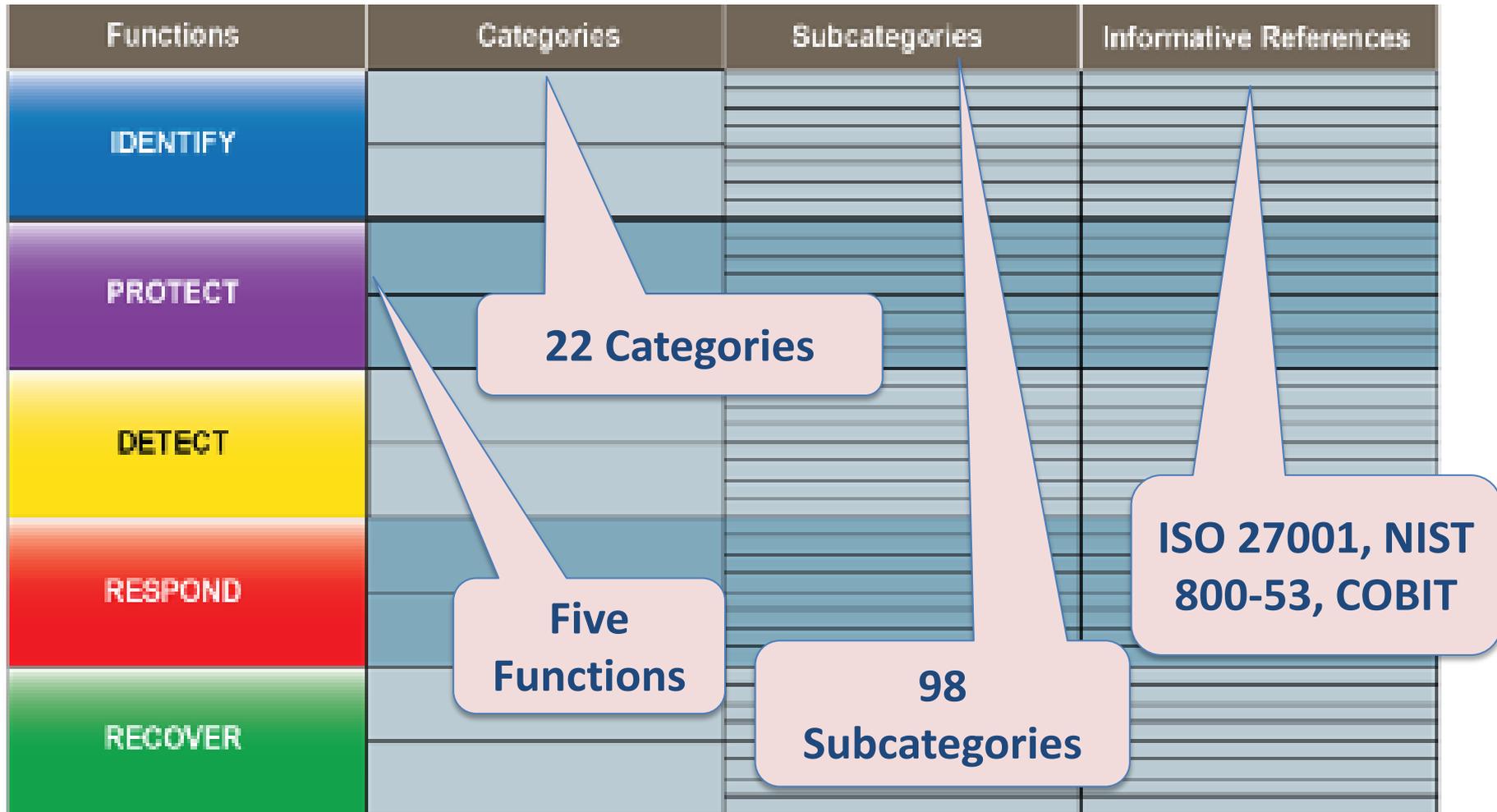


Figure 1: Framework Core Structure

Function ID	Function	Category ID	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 and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology

Function ID	Function	Category ID	Category
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

The Critical Infrastructure Cyber Community (C<sup>3</sup>) Voluntary Program focuses on three major activities:

**Supporting Use:** Assist stakeholders with understanding use of the Framework and other cyber risk management efforts, and support development of general and sector-specific guidance for Framework implementation.

**Outreach and Communications:** Serve as a point of contact and customer relationship manager to assist organizations with Framework use, and guide interested organizations and sectors to DHS and other public and private sector resources to support use of the Cybersecurity Framework.

**Feedback:** Encourage feedback from stakeholder organizations about their experience using C<sup>3</sup> Voluntary Program resources to implement the Framework. The C<sup>3</sup> Voluntary Program works with organizations to understand how they are using the Framework, and to receive feedback on how the Framework and the C<sup>3</sup> Voluntary Program can be improved to better serve organizations.

## (C<sup>3</sup>) Voluntary Program Resources

### **Cyber Resilience Review (CRR)**

The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals.

### **Cybersecurity Evaluation Tool (CSET) and On-Site Cybersecurity Consulting**

Industrial control systems security posture assessments, offered through CSET, a self-assessment tool. Features include a mapping to control systems standards based on the sector as well as a network architecture mapping tool.

### **Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT) Recommended Practices**

A list of recommended practices aimed at helping industry understand and prepare for ongoing and emerging control systems cybersecurity issues, vulnerabilities, and mitigation strategies.

## (C<sup>3</sup>) Voluntary Program Resources (Continued)

### **National Cyber Awareness System (NCAS)**

The National Cybersecurity and Communications Integration Center (NCCIC) produces advisories, alert & situation reports, analysis report, current activity updates, daily summaries, indicator bulletins, periodic newsletters, recommended practices, Weekly Analytic Synopsis Product (WASP), weekly digests, and year in review to alert partners of emerging cyber threats, vulnerabilities, and current activities.

### **U.S. Computer Emergency Readiness Team (US-CERT) and ICS-CERT**

Access to alerts, bulletins, tips, and technical documents published by ICS-CERT and US-CERT. ICS-CERT also offers an extensive bibliography of relevant standards and references.

### **Cyber Security Advisors (CSAs)**

CSAs are regionally located DHS personnel who direct coordination, outreach, and regional support to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's critical infrastructure and State, local, territorial, and tribal (SLTT) governments.

# Cybersecurity Risk Management Best Practices (WG 4)

## Cybersecurity Framework for the Communications Sector

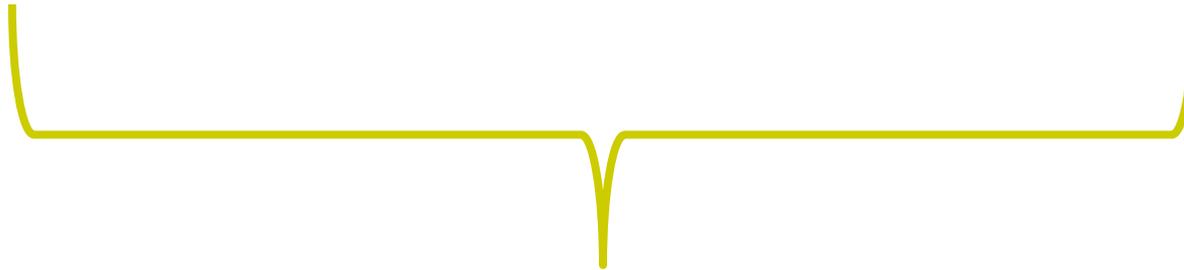
- ***Conform the NIST framework to the communications sector.*** Identify core mission(s), critical infrastructure and risks to the communications sector and organize the NIST core framework based on the aspects most relevant to ensuring the reliability and integrity of the core communications infrastructure.
- ***Maintain flexibility for individual companies.*** As part of this exercise based on updated threat information, and consistent with the NIST framework, the communications sector conforming framework will allow for flexibility for individual companies to self-determine how to apply the framework to their business based upon their own individual risk profile, risk tolerance, and critical infrastructure ownership.

- ***Develop new streamlined practices that follow Framework organization and common risk management approaches.*** Use existing CSRIC Best Practices and other resources to inform and organize the Framework with the goal to provide companies a “guide” of practices specific to communication segments that companies could elect to implement to mitigate cyber risk.
- ***Develop use cases/examples of how the framework is being used within the sector.*** Develop an appendix with illustrative examples or use cases about how the framework is being used or incorporated into risk management processes of communications companies. Descriptions will be anonymized and provide examples for all sector members around how aspects of the framework could be voluntarily used in the communications sector.
- ***Provide guidance to incorporate framework into existing company risk management processes.*** Determine high level processes that companies could perform, to the extent they use the framework, to incorporate it into their existing risk management program, or build a cyber risk management program where none exists today.



Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Figure 1: Framework Core Structure



## Communications Sector and Segment Risk Management Framework

Each industry segment reviews and updates best practices based on alignment with the Cybersecurity Framework design objectives

**Barriers To  
Implementation**

**Ecosystem Shared  
Responsibilities  
And Collaboration**

**Top Cyber Threats  
And  
Vectors**

**Small and Medium  
Business**

**NIST Version 1.0 Feedback**

## National Security Telecommunications Advisory Committee (NSTAC)

- Cloud Security
- Internet of Things
- NCCIC

## National Cybersecurity & Communications Integration Center (NCCIC)

- On call 24/7 center
- US CERT
- ICS CERT
- National Coordinating Center (NCC)



## Communications Sector Coordinating Council (CSCC) (DHS)

- Executive Order Implementation
- NIST Framework Implementation
- National Sector Risk Assessment (NSRA)
- Communications Sector Specific Plan (CSSP)
- National Incident Response Plan
- Emerging Security Framework (ESF)



## PRIMARY RESOURCES FOR CLE

1. Cybersecurity Executive Order 13636: Improving Critical Infrastructure Cybersecurity <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>
2. NIST Cybersecurity Framework: <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>
3. DHS Voluntary Program: <http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program>
4. FCC CSRIC: <http://www.fcc.gov/events/communications-security-reliability-and-interoperability-council-iv-meeting-0>

## ADDITIONAL RESOURCES

1. Critical Infrastructure Sector Partnerships  
<http://www.dhs.gov/critical-infrastructure-sector-partnerships>
2. National Infrastructure Protection Plan:  
<http://www.dhs.gov/national-infrastructure-protection-plan>
3. Critical Infrastructure Partnership Advisory Council:  
<http://www.dhs.gov/critical-infrastructure-partnership-advisory-council>