



NIST Standards in Trade Workshop with India on Information and Communication Technologies

Gaithersburg, Maryland
September 16, 2015

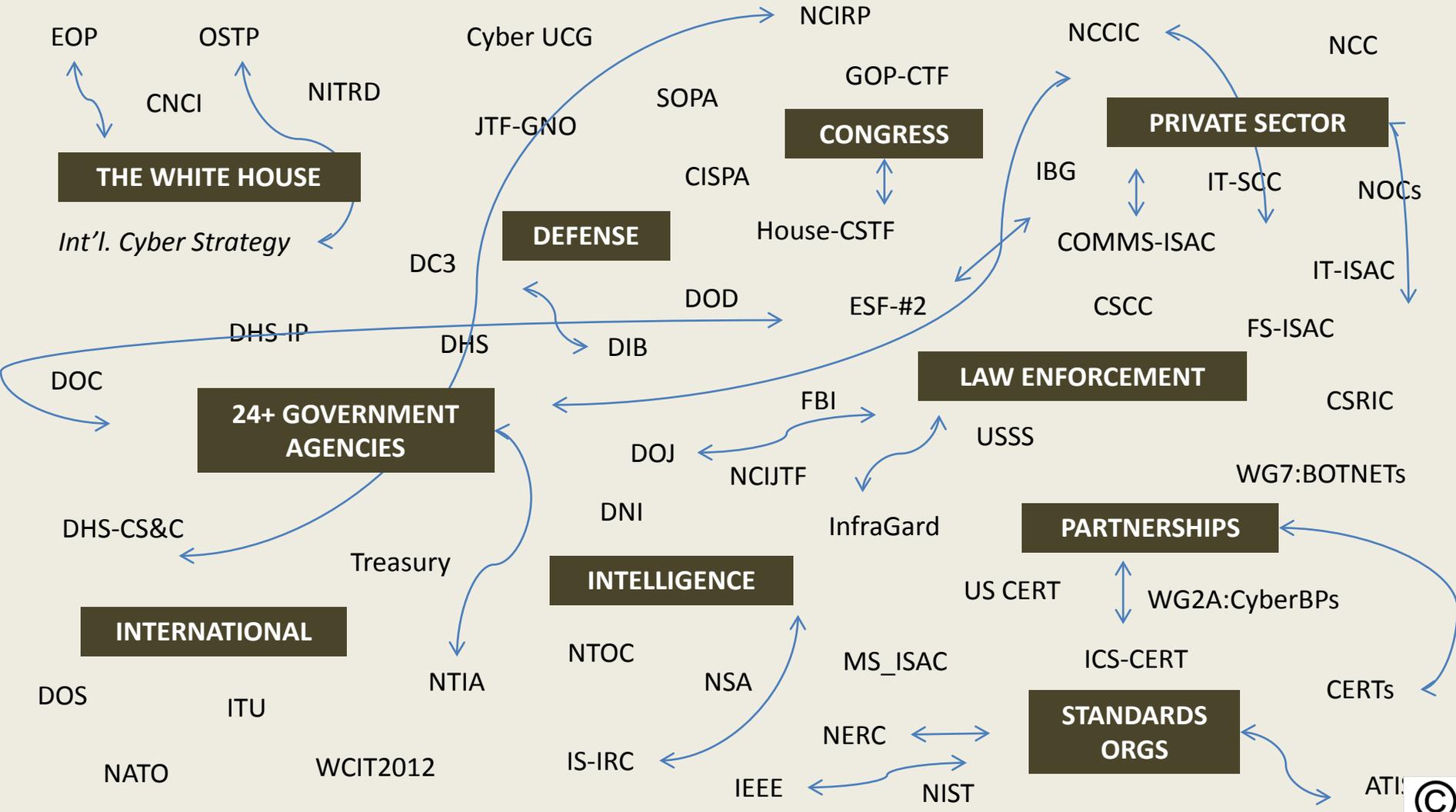


**Robert Mayer, Vice-President
Industry and State Affairs
United States Telecommunications
Association**

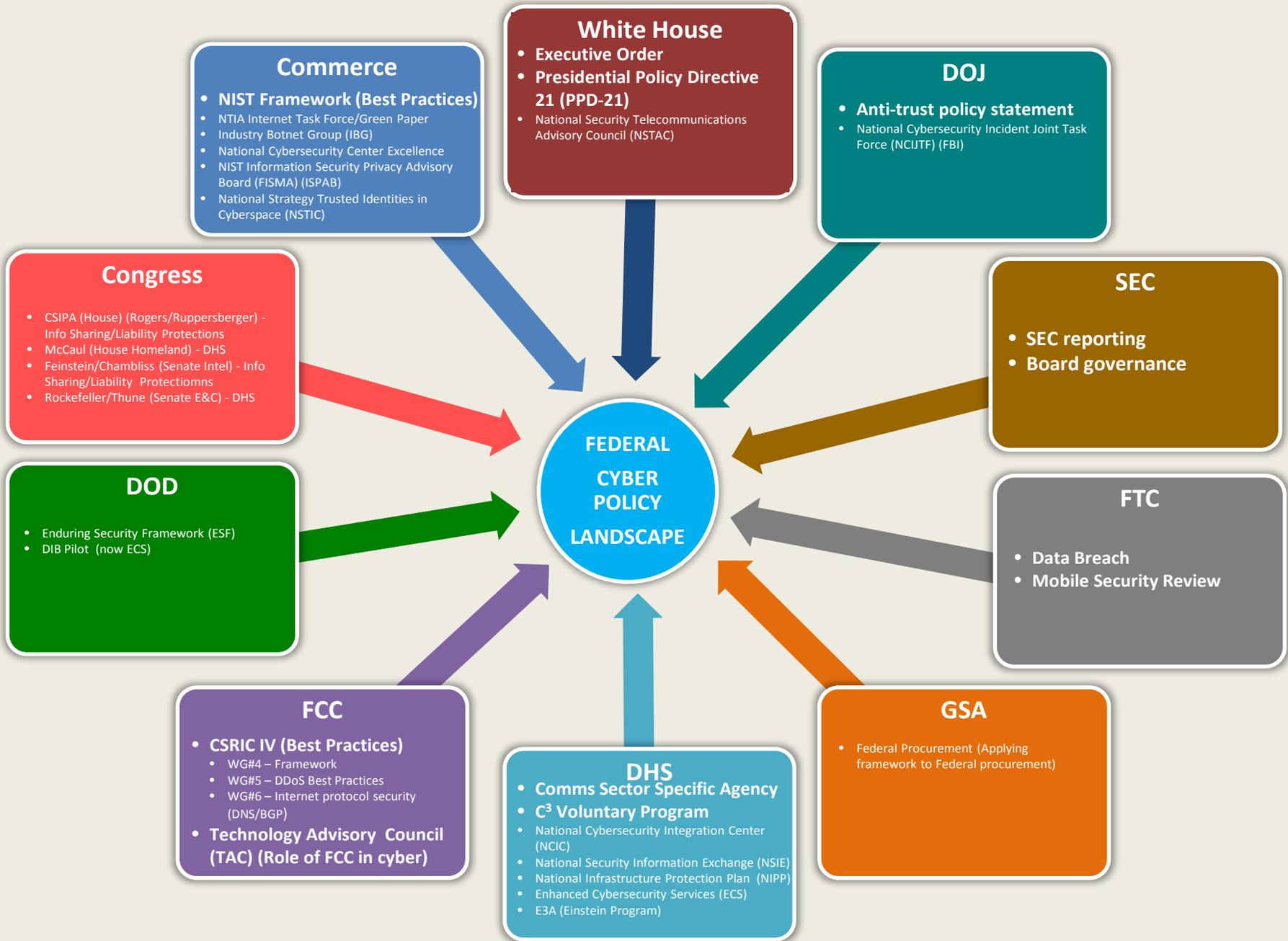


- Cybersecurity Landscape
- Public-Private Partnership Model
- Executive Order 13636
- NIST Framework Version 1.0
- FCC CSRIC IV – Working Group 4
- Discussion/Issues

Dynamic, Complex and Evolving Landscape



Federal Cybersecurity Policy Landscape



The Public-Private Partnership Operates on Multiple Levels



2013 Executive Order – Improving Critical Infrastructure Cybersecurity

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 13363
February 12, 2013



Standards for Critical Infrastructure

- NIST tasked with developing cross-sector framework, minimum security requirements for critical infrastructure.
- DHS tasked with establishing a voluntary program/ incentives to promote use (C³ program)
- Voluntary, non-regulatory – guideline for companies to build or complement risk management program
- Focused on critical infrastructure; however, Administration encouraging broader use.

DHS-led Information Sharing Program

- DHS to organize information sharing to rapidly distribute summaries of unclassified intelligence reports about known cyber threats.
- Expands Enhanced Cybersecurity Services (ECS) program to critical infrastructure.

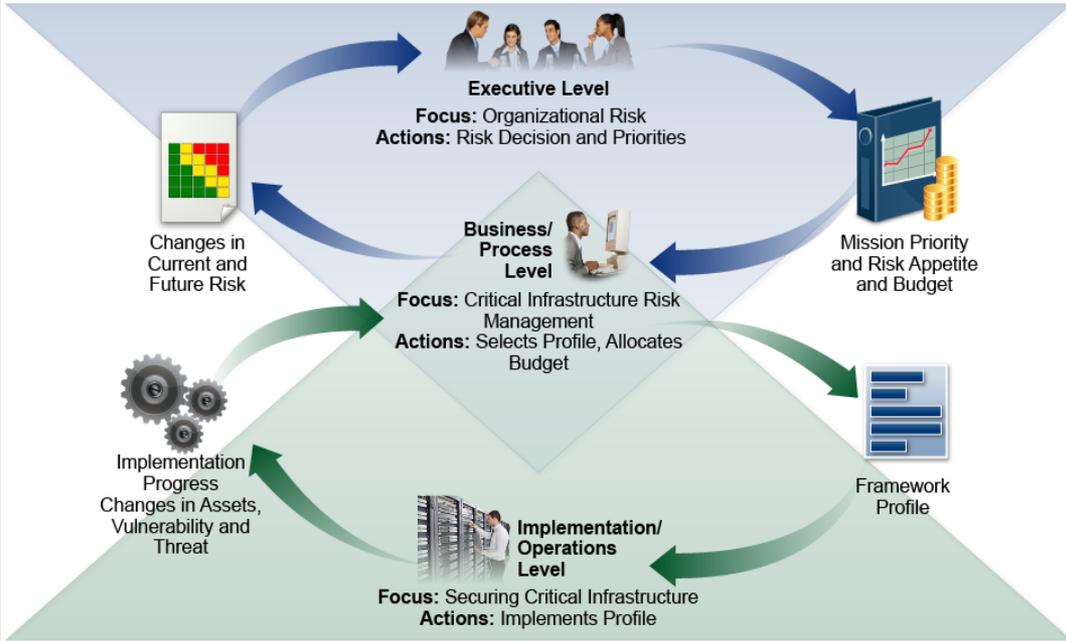
Regulators Review Authority

- DHS tasked with identifying critical infrastructure at greatest risk of cyber attack (Section 9).
- Regulators to examine how current regulatory frameworks address cybersecurity and harmonize existing regulations with practices identified by NIST.

NIST Framework for Improving Critical Infrastructure Cybersecurity

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. 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.

Risk Management



| Functions | Categories | Subcategories | Informative References |
|-----------|------------|---------------|------------------------|
| IDENTIFY | | | |
| PROTECT | | | |
| DETECT | | | |
| RESPOND | | | |
| RECOVER | | | |

Figure 1: Framework Core Structure

BROADCASTING



There are more than 14,000 radio and 1,700 television broadcasting facilities in the United States, sending broadcasts through the air to a frequency network of transmitters.

CABLE



The cable industry is composed of approximately 7,791 cable systems that offer analog and digital video programming services, digital telephone service, and high-speed Internet access service.

WIRELESS



Wireless technology consists of cellular phone, paging, personal communications services, high-frequency radio, unlicensed wireless and other commercial and private radio services.

WIRELIN



Over 1,000 companies offer wireline, facilities-based communications services in the United States. Wireline companies serve as the backbone of the Internet.

SATELLITE



Satellite communications systems deliver advanced data, voice, and video communications, transmitting data from one point on the Earth to another.

