RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Effects of Recent Federal Policies on Security and Resiliency Landscapes

SESSION ID: PNG-F03A

Dr. Nader Mehravari

Resilience Management Team
Software Engineering Institute
Carnegie Mellon University
nmehravari@sei.cmu.edu

Session Abstract

Recent executive orders, presidential policy directives, and federal agency activities are affecting strategies and practices for cybersecurity protection and resilience of the nation's critical infrastructure.

- What are they?
- How are they related to previous such actions?
- How are they affecting cybersecurity and resilience strategies of owners and operators of nation's critical infrastructure?
- What is the role of federal government in responding cyber attacks?

Setting the Stage

- What policy developments took place in February 2013?
- Why are these developments important?

Developments During the Week of Feb. 12, 2013

President's State of Union Address

Executive Order

*(Improving **Critical Infrastructure** Cybersecurity)*

Presidential Policy Directive – PPD 21

*(Critical Infrastructure **Security and Resilience**)*

NIST's Plans for Development of a **Cybersecurity Framework**

Why are these developments important?

In the past, there have been Executive Orders , Presidential Policy Directives, and/or legislative actions with major effects on:

- Disaster planning
- Crisis management
- Identity management
- Emergency communications
- Critical infrastructure protection
- Application of DR/BC/InfoSec national & int'l standards

Conditions are "ripe" for the recent policy developments to significantly affect cybersecurity and resiliency landscapes.

Historical Background

- Source of Federal Regulations
- Congressional Activities
- Presidential Executive Orders
- Presidential Policy Directive

Sources of Federal Regulations

In the United States, cybersecurity and resiliency **regulation** comprises:

Legislation
from Congress

Directives
from the Executive Branch

Congressional Cybersecurity Activities

- Congress has been holding hearings related to cybersecurity every year since 2001

Number of bills and resolutions introduced with provisions related to cybersecurity	
111th Congress *(January 2009 – January 2011)*	60+
112th Congress *(January 2011 – January 2013)*	40+
113th Congress (as of May 22, 2013)	17

No comprehensive cybersecurity legislation has been enacted since 2002.

What are Presidential Executive Orders?

- United States Presidents issue executive orders to help officers and agencies of the executive branch manage the operations within the federal government itself.
- **Executive orders have the full force of law.**
- Certain executive orders focus on national security issues.

Some Key Examples

Year	Administration	Created
1963	JF Kennedy	National Communications Systems (NCS)
1984	R Reagan	Gov't Emergency Telecom. Service (GETS)
2002	GW Bush	Department of Homeland Security
2003	GW Bush	HSPD-7: National Infrastructure Protection Plan (NIPP)
2006	GW Bush	Integrated Public Alert and Warning System (IPAWS)

Description of February 2013 Policy Developments

- Executive Order No. 13636
- Presidential Policy Directive PPD-21
- NIST Initiating Development of a Cybersecurity Framework

EO # 13636 and PPD #21

	Executive Order 13636	Presidential Policy Directive PPD-21
		
Issuance Date	Tuesday, February, 12, 2013	
Title	Improving Critical Infrastructure Cybersecurity	Critical Infrastructure Security and Resilience
Overall Objective	**To enhance the security and resilience of the Nation's critical infrastructure**	
Classification	Unclassified	

Messages of Executive Order & PPD

"…Our country's reliance on cyber systems to run everything from power plants to pipelines and hospitals to highways has increased dramatically, and our infrastructure is more physically and digitally interconnected than ever…"

"…The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront…"

"…Steps must be taken to enhance existing efforts to increase the protection and resilience of critical infrastructure, while maintaining a cyber environment that encourages efficiency, innovation, and economic prosperity, while protecting privacy and civil liberties…"

Overall Objectives of EO and PPD

To strengthen the security and resilience of critical infrastructure against evolving threats through an updated and overarching national framework that acknowledges the increased role of cybersecurity in securing physical assets.

Together, the EO and PPD create an opportunity to reinforce the need for holistic thinking about security risk management and drive action toward a whole of community approach to security and resilience.

NIST Framework Development Process

- February 2013 – NIST Issues RFI
- April 3, 2013 – 1st Framework Workshop
- April 8, 2013 – RFI Responses Posted
- May 15, 2013 – Identify Common Practices/Themes
- May 29-31, 2013 – 2nd Framework Workshop
- June 2013 – Draft Initial Framework
- July 2013 – 3rd Framework Workshop
- September 2013 – 4th Framework Workshop
- October 2013 – Publish Preliminary Framework
- November 2013 – 5th Framework Workshop
- December 2013 – Public comment period
- February 2014 – Release Official Framework

Closing Thoughts

Observation:

- Taking Actions “Before” & “After” major national disruptive events

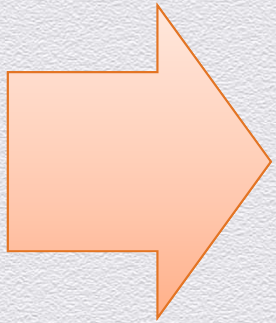
- After Cuban Missile Crisis
  - Presidential Memorandum of August 21, 1963 (NCS)
- After September 11
  - HSPD 1, 5, 7, 8, 12, 20, 21
  - Homeland Security Act of 2002
  - PS-PREP
- After Mailings of Anthrax Spores
  Homeland Security Act of 2002 (DHS)
- After Hurricane Katrina
  - EO-13407 (IPAWS)

- PPD-63 (CIP)
- EO-13636 and PPD-21 (CI Security and Resilience)

Observation:

- PPD-21 accounts for:
  - new risk environment
  - key lessons learned
  - drive toward enhanced capabilities

HSPD-7
Terrorist Attacks
Physical Systems



PPD-21
Security & Resilience of CI (protection + operating under stress)
All hazards
Recognizes CI cybersecurity a matter of national security

Question: Enable active defenses?

- An active shooter in a bank lobby would likely meet deadly force in response
- Should organizations be legally allowed to fight back when under cyber attack?
- Do we need policies and regulations governing such active cyber defenses?

Question: National defenses

- If a foreign state fired a missile at a US bank HQ, it would meet immediate military defense
- Should military-grade cyber defenses be deployed to protect US businesses that are under attack by foreign states?
- Do we need another exception to the Posse Comitatus Act to enable military cyber response to large-scale cyber attacks on US critical infrastructure?

Thank you for your attention…