Recent Federal Policies Affecting the Cybersecurity and Resiliency Landscape

Nader Mehravari
Research Scientist, CERT® Division

Dr. Nader Mehravari is with the CERT® Program at the Software Engineering Institute (SEI), a unit of Carnegie Mellon University in Pittsburgh, PA. His current areas of interest and research include operational resilience, protection and sustainment of critical infrastructure, preparedness planning, and associated risk management principles and practices.

Nader was with Lockheed Martin from 1992 through 2011. In his most recent assignment, he was the Director for Business Resiliency. In this capacity, he led and oversaw all preparedness planning and associated governance and compliance activities. He was responsible for building and leading Lockheed Martin's resiliency program where he successfully implemented a modern, integrated, risk management based approach to disaster recovery, business continuity, pandemic planning, crisis management, emergency management, and workforce continuity for all of Lockheed Martin.
Outline

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

Some Historical Background Relevant to Cybersecurity & Resilience
- Source of Federal Regulations
- Existing Federal Regulations
- Congressional Activities
- Presidential Executive Orders
- Presidential Policy Directive

Description of the February 2013 Developments
- Executive Order No. 13636
- Presidential Policy Directive (PPD) 21
- NIST Initiating Development of a Cybersecurity Framework

Closing Thoughts
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 the Union Address
- Executive Order (Improving Critical Infrastructure Cybersecurity)
- Presidential Policy Directive – PPD 21 (Critical Infrastructure Security and Resilience)
- NIST’s Plans for Developing a Cybersecurity Framework
Why are these developments important?

“...85 percent of our nation’s critical infrastructure is controlled not by government but by the private sector...”

—The 9/11 Commission Report
Critical Infrastructure

“… 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 …”

—Title 42, Code of Laws of the United States of America
Why are these developments important?

“... the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents...”

—Presidential Policy Directive – PPD 21
(February 12, 2013)
Critical Infrastructure Sectors

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Health Care and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems
Kinetic Disruptions to Critical Infrastructure
Cybersecurity Disruptions to Critical Infrastructure

More companies reporting cybersecurity incidents

By Ellen Nakashima and Danielle Douglas, Published: March 1

At least 19 financial institutions have disclosed that computers were targets of malicious cyberattacks, with some institutions reporting multiple incidents. The attacks, which include banking and insurance companies, have reported losing $100 million in revenues.

In their annual financial report, banks such as Bank of America, JPMorgan Chase, and Wells Fargo, have reported increased cybersecurity expenses in recent years. These expenses include hiring more cybersecurity professionals, investing in new technologies to protect against cyber attacks, and conducting more training for employees.

The cyber attacks have targeted numerous sectors, including banking, energy, transportation, and telecommunications. The attacks have disrupted services to consumers and have required organizations to invest in new technologies to protect against future attacks.

Gartner.

Why Gartner | About Gartner

Are the cyber attacks just the beginning?

by Avivah Litan

That’s a viable hypothesis, but the number of bots they had staged at a single point in time on Tuesday. Reportedly, on Tuesday the total number of bots at one point in time on the largest attack against a single bank at 110 gigabits.

Interestingly, the attackers could have easily done even more damage but they chose not to. 9200 bots were identified as attack-capable but the total number of bots actually involved in sending the DDoS traffic to the banks numbered only about 3200. The other 6000 bots sat there doing nothing.

CERT Operational Resilience: Manage, Protect, and Sustain
Twitter #CERTopRES
© 2014 Carnegie Mellon University
Why are these developments important?

In the past, there have been executive orders, presidential policy directives, and legislative actions with major effects on

- disaster planning
- crisis management
- identity management
- emergency communications
- critical infrastructure protection
- application of DR/BC/InfoSec national & international standards

Conditions are ripe for recent policy developments to significantly affect cybersecurity and resiliency landscapes.
Historical Background

- Source of Federal Regulations
- Existing 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*
Existing Federal Regulations

There are few cybersecurity and resiliency regulations. The ones that exist focus on specific industries.

The three main existing cybersecurity regulations are

<table>
<thead>
<tr>
<th>1996 Health Insurance Portability and Accountability Act</th>
<th>Health Care Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1999 Gramm–Leach–Bliley Act</td>
<td>Financial Institutions</td>
</tr>
<tr>
<td>2002 Homeland Security Act, which included the Federal Information Security Management Act (FISMA)</td>
<td>Federal Agencies</td>
</tr>
</tbody>
</table>
Congressional Cybersecurity Activities

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

Most recently:

<table>
<thead>
<tr>
<th>Congress</th>
<th>Number of Bills and Resolutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>111th Congress</td>
<td>60+</td>
</tr>
<tr>
<td>(January 2009 – January 2011)</td>
<td></td>
</tr>
<tr>
<td>112th Congress</td>
<td>40+</td>
</tr>
<tr>
<td>(January 2011 – January 2013)</td>
<td></td>
</tr>
<tr>
<td>113th Congress</td>
<td>17</td>
</tr>
<tr>
<td>(as of May 22, 2013)</td>
<td></td>
</tr>
</tbody>
</table>
Cybersecurity Legislation

The Obama Administration sent Congress a package of legislative proposals in May 2011

• to give the federal government new authority to ensure that corporations that own the assets most critical to the nation’s security and economic prosperity are adequately addressing the risks posed by cybersecurity threats.

No comprehensive cybersecurity legislation has been enacted since 2002.
What Are Presidential Executive Orders?

U.S. presidents issue executive orders to help officers and agencies of the executive branch manage the operations within the federal government.

What Are Presidential Executive Orders?

Executive orders have the full force of law.

Typically made in pursuance of certain acts of Congress, some of which specifically delegate to the president some degree of discretionary power.

Or are believed to take authority from power granted directly to the executive by the Constitution.
What Are Presidential Directives?

A form of an executive order issued by the president of the United States

- with the advice and consent of the National Security Council

Articulate the executive's national security policy.

They carry the full force and effect of law.

Since many presidential directives pertain to the national security of the United States, many are classified.
Presidential Memorandum, August 21, 1963

President Kennedy established the National Communications System (NCS)

After the Cuban missile crisis

The NCS mandate included linking, improving, and extending the communications facilities and components of various federal agencies, focusing on interconnectivity and survivability.
E.O. 12472 - April 3, 1984

Assignment of National Security and Emergency Preparedness Telecommunications Functions

Superseded President Kennedy’s original 1963 memorandum

Broadened the NCS
Critical Infrastructure Protection

Set national goal:

- The ability to protect the nation’s critical infrastructure from intentional attacks
- Any interruptions in the ability of these infrastructures to provide their goods and services must be “brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.”
Homeland Security Act of 2002

Was introduced in the aftermath of

- September 11 attacks
- mailings of anthrax spores

Established the

- Department of Homeland Security (DHS)
- cabinet-level position of secretary of homeland security
HSPD-7 – December 7, 2003

Critical Infrastructure Identification, Prioritization, and Protection

Replaced PPD-63

Aimed to unify protection efforts for critical infrastructure and key resources (CIKRs) across the country

Focus of HSPD-7

<table>
<thead>
<tr>
<th>Terrorist attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical systems</td>
</tr>
</tbody>
</table>
E.O. 13407 - June 26, 2006

Public Alert and Warning System

Following Hurricane Katrina

Ordered DHS to establish a new program to integrate and modernize the nation's existing population warning systems, such as

- Emergency Alert System (EAS)
- National Warning System (NAWAS)
- Commercial Mobile Alert System (CMAS)
- NOAA Weather Radio All Hazards

Subsequently termed the Integrated Public Alert and Warning System (IPAWS)
Description of February 2013 Policy Developments

• Executive Order No. 13636
• Presidential Policy Directive (PPD) 21
• NIST Initiated Development of a Cybersecurity Framework
Executive Order

Executive Order No.

• 13636

Issuance Date

• Tuesday, February 12, 2013

Title

• Improving Critical Infrastructure Cybersecurity

Overall Objective

• To enhance the security and resilience of the nation's critical infrastructure

Classification

• Unclassified
Presidential Policy Directive

  • PPD-21

Issuance Date
  • Tuesday, February 12, 2013

Title
  • Critical Infrastructure Security and Resilience

Classification
  • Unclassified
“...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.
Sections of the Executive Order

- Policy
- Critical Infrastructure
- Policy Coordination
- Cybersecurity Information Sharing
- Privacy and Civil Liberties Protections
- Consultative Process
- Baseline Framework to Reduce Risk to Critical Infrastructure
- Voluntary Critical Infrastructure Cybersecurity Program
- Identification of Critical Infrastructure at Greatest Risk
- Adoption of Framework

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.
Sections of the Executive Order

- Policy
- Critical Infrastructure
- Policy Coordination
- Cybersecurity Information Sharing
- Privacy and Civil Liberties Protection
- Consultative Process
- Baseline Framework to Reduce Risk to Critical Infrastructure
- Voluntary Critical Infrastructure Cybersecurity Program
- Identification of Critical Infrastructure at Greatest Risk
- Adoption of Framework

DHS to establish a new information sharing program to provide both classified and unclassified threat and attack information to U.S. companies
Sections of the Executive Order

- Policy
- Critical Infrastructure
- Policy Coordination
- Cybersecurity Information Sharing
- Privacy and Civil Liberties Protections
- Consultative Process
- Baseline Framework to Reduce Risk to Critical Infrastructure
- Voluntary Critical Infrastructure Cybersecurity Program
- Identification of Critical Infrastructure at Greatest Risk
- Adoption of Framework

*Agencies are required to incorporate privacy and civil liberties safeguards in their cybersecurity activities.*
Sections of the Executive Order

- Policy
- Critical Infrastructure
- Policy Coordination
- Cybersecurity Information Sharing
- Privacy and Civil Liberties Protections
- Consultative Process
- Baseline Framework to Reduce Risk to Critical Infrastructure
- Voluntary Critical Infrastructure Cybersecurity Program
- Identification of Critical Infrastructure at Greatest Risk
- Adoption of Framework

NIST to lead the development of a Cybersecurity Framework to reduce risk to critical infrastructure
Sections of Presidential Policy Directive

Introduction
Policy
Roles and Responsibilities
Three Strategic Imperatives
Innovation and Research
Implementation of the Directive
Designated Critical Infrastructure Sectors and Specific Agencies
Definitions

Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards.

This directive establishes national policy on critical infrastructure security and resilience.
## Sections of Presidential Policy Directive

| Introduction |
| Policy |
| Roles and Responsibilities |
| Three Strategic Imperatives |
| Innovation and Research and Development |
| Implementation of the Directive |
| Designated Critical Infrastructure Sectors and Sector-Specific Agencies |
| Definitions |

**Address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect this infrastructure's interconnectedness and interdependency.**
Sections of Presidential Policy Directive

- Introduction
- Policy
- Roles and Responsibilities
- Three Strategic Imperatives
- Innovation and Research and Development
- Implementation of the Directive
- Designated Critical Infrastructure Sectors and Sector-Specific Agencies
- Definitions

Calls for a comprehensive R&D plan for critical infrastructure to guide the government’s effort to enhance and encourage market-based innovation.
Sections of Presidential Policy Directive

Introduction
Policy
Roles and Responsibilities
Three Strategic Imperatives
Innovation and Research and Development
Implementation of the Directive
Designated Critical Infrastructure Sectors and Specific Agencies
Definitions

1. Chemical
2. Commercial Facilities
3. Communications
4. Critical Manufacturing
5. Dams
6. Defense Industrial Base
7. Emergency Services
8. Energy
9. Financial Services
10. Food and Agriculture
11. Government Facilities
12. Health Care and Public Health
13. Information Technology
14. Nuclear Reactors, Materials, & Waste
15. Transportation Systems
16. Water and Wastewater Systems
RESILIENCE ... the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

ALL HAZARDS ... natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.
PPD-21 Replaces HSPD-7 of 2003

To account for

- new risk environment
- key lessons learned
- drive toward enhanced capabilities

---

<table>
<thead>
<tr>
<th>HSPD-7</th>
<th>PPD-21</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terrorist attacks</td>
<td>Security &amp; resilience of CI (protection + operating under stress)</td>
</tr>
<tr>
<td>Physical systems</td>
<td>All hazards</td>
</tr>
<tr>
<td></td>
<td>Recognizes that CI cybersecurity is a matter of national security</td>
</tr>
</tbody>
</table>
Aspects of OE/PPD Related to Framework

NIST shall

- develop a cybersecurity framework (CSF)

DHS shall

- establish a voluntary program to promote the adoption of the CSF

Regulatory agencies shall

- review the framework and determine if current regulations are sufficient
- develop new regulations if current ones are insufficient
NIST Framework Development Process

- Engage the Framework Stakeholders
- Collect, Categorize, & Post RFI Responses
- Analyze RFI Responses
- Select Framework Components
- Prepare & Publish Preliminary Framework
- Release Official Framework

- February 2013 – NIST Issues RFI
- April 3, 2013 – 1st Framework Workshop
- April 8, 2013 – Post RFI Responses
- 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

<table>
<thead>
<tr>
<th>HSPD-7</th>
<th>PPD-21</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terrorist attacks</td>
<td>Security &amp; resilience of CI (protection + operating under stress)</td>
</tr>
<tr>
<td>Physical systems</td>
<td>All hazards</td>
</tr>
<tr>
<td></td>
<td>Recognizes that CI cybersecurity is a matter of national security</td>
</tr>
</tbody>
</table>
Observation (& Question to Be Considered)

Policies and doctrines around kinetic attacks on U.S. interests are mature, but they fail to provide needed clarity when applied to cyber-based attacks, especially those of foreign state actors.

For example…
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?
U.S., Firms Draw a Bead on Chinese Cyberspies

By DANNY YADRON and SIOBHAN GORMAN

The U.S. government gave American Internet providers addresses linked to suspected Chinese hackers earlier this year as part of a previously undisclosed effort aimed at blocking cyberspying, current and former U.S. officials said.

The push reflects a significant shift in levels of cooperation between the

The efforts represent a rare glimpse into what NSA Director Gen. Keith Alexander and other officials call "active defense," which they characterize as exercising self-defense in cyberspace. How such activities are executed remains largely cloaked in mystery.
Question: National Defenses

If a foreign state fired a missile at a U.S. bank HQ, it would meet immediate military defense.

Should military-grade cyber defenses be deployed to protect U.S. 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 U.S. critical infrastructure?
Role of Federal Government?

Should Companies Be Required to Meet Certain Minimum Cybersecurity Protections?

By SIOBHAN GORMAN

U.S. companies appear to have lots of not-so-secret secrets.

Intelligence reports, for instance, say China and Russia have been pilfering vast quantities of secrets from U.S. companies, while U.S. officials say Iranian-backed hackers have mounted a relentless campaign against U.S. banks.

President Barack Obama in February.
A Call to Arms for Banks

Regulators Intensify Push for Firms to Better Protect Against Cyberattacks

By MICHAEL R. CRITTENDEN

WASHINGTON—U.S. regulators are stepping up calls for banks to better-arm themselves against the growing online threat hackers and criminal organizations pose to individual institutions and the financial system as a whole.

The push comes as government officials grow increasingly concerned about the ability of a cyber attack to cause significant disruptions to the financial system. Banks such as J.P. Morgan Chase & Co., Bank of America Corp. (BAC +0.73%) and Capital One Financial Corp. (COF +0.70%) have been targeted by cyber assaults in recent years, including potent "denial-of-service" strikes that took down some bank websites or forced customers to visit physical locations. Banks have spent millions of dollars...
References

Specific to the Executive Order

- https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

Specific to PPD-21

- http://www.hsdl.org/?abstract&did=731087

Specific to NIST Framework

- https://www.federalregister.gov/articles/2013/02/26/2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity#h-4

Other References

As projects continue to grow in scale and complexity, effective collaboration across geographical, cultural, and technical boundaries is increasingly prevalent and essential to system success. SATURN 2012 will explore the theme of "Architecture: Catalyst for Collaboration."

Introduction to the CERT Resilience Management Model
February 18 - 20, 2014 (SEI, Arlington, VA)
June 17 - 19, 2014 (SEI, Pittsburgh, PA)
See Materials Widget for course document