Deloitte.

Succeeding in a cyber world

Kentucky Digital Government Summit

Harry D. Raduege, Jr.
Lieutenant General, (USAF, Ret)
Chairman, Deloitte Center for Cyber Innovation

April 23, 2013

The world of cybersecurity

Threats

- Identity theft
- Information manipulation (e.g. Malware)
- Cyber Assaults/Bullying
- Advanced Persistent Threats (APTs)
- Information theft
- Crime (e.g. Credit card fraud)
- Insider
- Espionage
- Cyber attack
- Transnational
- Attack of software "boomerangs"
- Terrorism

Targets

- Government (Federal, State and Local); e.g.,
  - E-Government
  - E-Commerce
- Industry; e.g.,
  - Aerospace & Defense
  - Banking & finance
  - Health care
  - Insurance
  - Manufacturing
  - Oil & Gas
  - Power Grid
  - Retail
  - Telecommunications
  - Utilities
- Universities/Colleges
- Individuals

Counters

- Cyber workforce
- Network access controls
  - Firewalls
  - Anti-virus S/W
  - S/W patch management
  - ID management
- Outbound traffic monitoring
- Dynamic situational awareness
- Open source Information
- Risk intelligence & management
  - Data analytics
- Forensic analysis
- Financial intelligence (FININT)
- Tighter laws & enforcement ties
- Expanded diplomacy
- Legislation?

You should assume that your network has or will be compromised.

What global experts are thinking about cybersecurity…

54% doubt their organization is capable of defending itself against a sophisticated cyber attack

61% anticipate the impact of losing global connectivity for an extended period of time to be catastrophic with irreversible consequences

66% think home users need to take more responsibility for cybersecurity

66% view their government's maturity as low regarding international cooperation

66% a "treaty on cyber warfare" is needed or is overdue

69% doubt their country could defend against a sophisticated cyber attack

70% believe that international policies and regulations are far behind technology advances

"Protecting the Digital Economy", East West Institute Report from the First Worldwide Cybersecurity Summit , May 2010

"Mobilizing for International Action", EastWest Institute Report from the Second Worldwide Cybersecurity Summit, June 2011

State Governments Are a Target

- States have the most comprehensive information about citizens; for this reason, organized cyber criminals have targeted government and higher education agencies for the past few years.
  - Data loss from government impacts citizen trust and has the potential to impact state business by affecting citizen services, revenue collections, or unplanned spending
- In recent months, there has been an increase in high-profile cyber attacks from loose-knit, politically-motivated groups operating globally.

  - These groups are distinct from more well established cyber criminal organizations, in both organizational structure (ad-hoc vs. top-down) and motivation (“hacktivism” vs. monetary gain).
- Recent developments have elevated Cybersecurity to a Governor level issue.

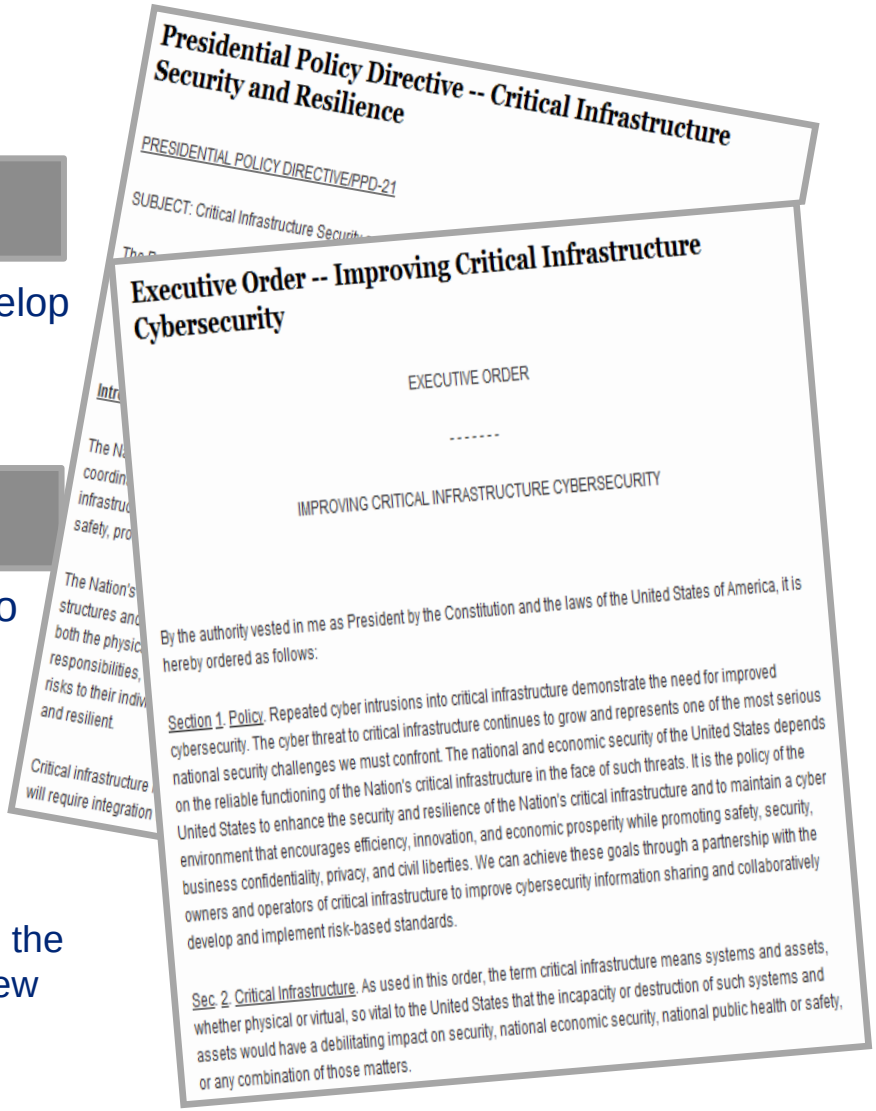
President Obama's Executive Order on "Improving Critical Infrastructure Cybersecurity" & PPD-21 (February 12, 2013)

Goal

- Improve cybersecurity information sharing and develop and implement risk-based critical infrastructure standards through a public-private partnership.

Key Takeaways

- Increase information sharing from government to private sector
- Develop Standards
  - NIST leading public-private collaboration to build Cybersecurity Framework
- Identify Critical Infrastructure
  - Uses a lower threshold for critical infrastructure than the standard definition (catastrophic regional/national view versus the standard "debilitating impact")



Presidential Policy Directive -- Critical Infrastructure Security and Resilience

PRESIDENTIAL POLICY DIRECTIVE/PPD-21

SUBJECT: Critical Infrastructure Security

Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. 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.

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.

The new E.O. changes the definition of “critical infrastructure”

The new E.O. defines **“critical infrastructure at greatest risk,”** as infrastructure where “a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.”

Executive Order,
Improving Critical Infrastructure Cybersecurity, Section 9

Key milestones of the Executive Order

	Near-term	Mid-term	Long-term
	< 150 days	150 days to 1 year	1+ years
Private Sector	• Partner to shape development of a cybersecurity framework • Dialogue on information sharing	• New companies identified as “critical infrastructure” • Identify Cybersecurity Framework leader	• Adopt the Cybersecurity Framework • Report on impact of requirements (2 years)
Public Sector	• Broaden information-sharing process, assess privacy risks, analyze incentives (120 days) • Expand on enhanced Cybersecurity Services (120 days) • Establish voluntary program to support Framework adoption (120 days)	• Identify critical infrastructure at greatest risk • Review and comment on Cybersecurity Framework • Develop a preliminary Framework (240 days) • Look for funding and budget opportunities to implement Cybersecurity Framework	• Issue final Framework (1 year) • Report program participation and privacy risks (annually) • Review, update CI list (annually) • Report *if* current regulatory requirements are insufficient • Report on CI impacts (2 years)

Critical Infrastructure Cybersecurity - Executive Order (EO) and Presidential Policy Directive (PPD-21)
State/local government impact

1. Federal Department of Homeland Security and a few federal agencies are responsible for most of the direct actions resulting from the EO and Presidential Policy Directive
   - State homeland security agencies are likely to play a pivotal information sharing role for government and commercial sector

2. State/local government agencies coming under the critical infrastructure definition will look for funding opportunities from the federal government to implement the Cybersecurity Framework
   - Transportation (mass transit, highways, bridges, airports)
   - Health (disease management, health information exchanges),
   - Public safety (emergency management, law enforcement), and
   - Utilities (nuclear/power/chemical plants)

3. Most states have not adopted or implemented a security framework and the EO will be a catalyst for them to consider embracing the Cybersecurity Framework

4. *Unrelated to the EO/PPD, NGA has formed a "National Policy council for State Cybersecurity". Deloitte is a participant and will help shape policy recommendations for state governors on Cybersecurity*

Currently, there are 16 industry sectors defined as critical infrastructure

85% of critical infrastructure is in private sector hands[1]

Trends exposing industry to increased risk

- Interconnectedness of sectors
- Proliferation of exposure points
- Concentration of assets

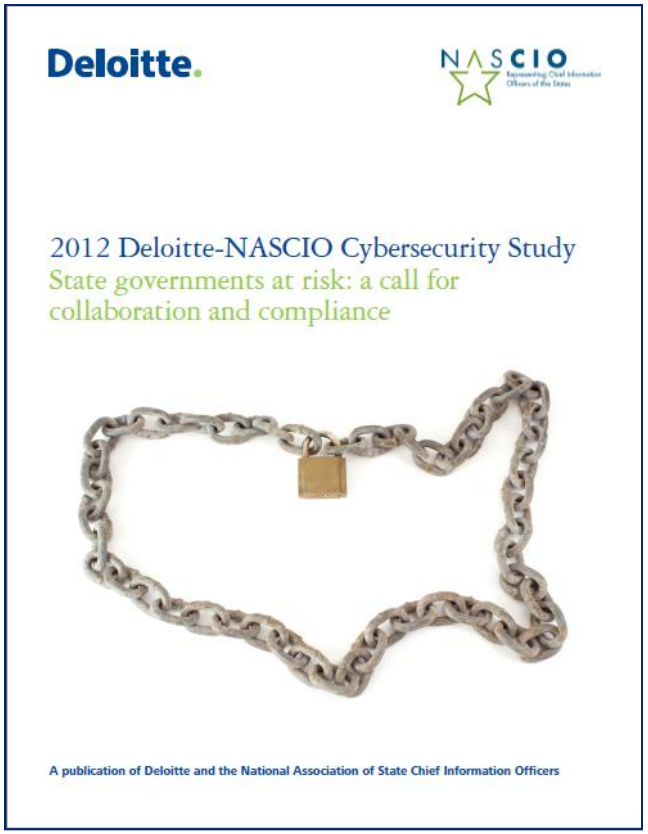
Critical infrastructure sectors		
Agriculture and Food	Dams	Information Technology
Banking and Financial Services	Defense Industrial Base	Nuclear Reactors, Materials and Waste
Chemical	Emergency Services	Transportation Systems
Commercial Facilities	Energy	Water and Wastewater Systems
Communications	Government Facilities	Critical Manufacturing
	Healthcare and Public Health	

1 GAO Report, Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve. July 2007, http://www.gao.gov/assets/100/95010.pdf

2012 Deloitte – NASCIO Cybersecurity Study Survey Results and Timeline

Survey results

- 2012 Deloitte –NASCIO Cybersecurity Study – Available in print and electronic format – Downloadable from www.nascio.org and www.deloitte.com.
- One confidential benchmark report for every state CISO respondent – comparing their individual survey responses with the aggregated survey results.



Report : State Governments at risk: A call for collaboration and compliance

Cybersecurity State Roadmap

*Source: State Governments at risk: A call for collaboration and compliance