

# Legal and Regulatory Developments for Privacy and Security

---

Rodney Petersen

Government Relations Officer and  
Director of EDUCAUSE Cybersecurity Initiative



# Overview

---

- Context for Federal Policy
- Policy Directions
  - Executive Branch
  - Legislative Branch
  - Regulatory Agencies
- Implementation of Higher Ed Opportunities Act
- Higher Education Information Security Council
- Campus Safety & Security
- Discussion



# Priorities in Washington

---

- Economy
- Economy
- Economy
- Swine Flu
- Healthcare Reform



# Higher Education Policy

---

- Student Aid
- Economic Stimulus
- Research Funding
- Access
- Affordability
- Accountability



# Presidential Pronouncements on Cybersecurity

---

- 1998: PDD-63 – Critical Infrastructure Protection
- 2003: National Strategy to Secure Cyberspace
- 2004: HSPD-7 – Critical Infrastructure Identification, Prioritization, and Protection
- 2007: Comprehensive National Cybersecurity Initiative (CNCI)
- 2009: Cybersecurity Policy Review



# Cyberspace Policy Review

---

- Summary of the Problem: Cybersecurity risks pose some of the most serious economic and national security challenges of the 21<sup>st</sup> century.
- Goal: Maintaining a information and communications infrastructure that promotes efficiency, innovation, economic prosperity, and free trade while also promoting safety, security, civil liberties, and privacy rights.



# Components of Report

---

- Leading from the Top
- Building Capacity for a Digital Nation
- Sharing Responsibility for Cybersecurity
- Creating Effective Information Sharing and Response
- Encouraging Innovation



# White House Leadership

---

- Finding: no single individual or entity has the responsibility to coordinate Federal government cybersecurity-related activities.
- Solution: anchoring and elevating leadership for cybersecurity-related policies at the White House signals to the United States and the international community that we are serious about cybersecurity.
- Approach: appoint a cybersecurity policy official with ties to the National Security Council & the National Economic Council



# Building Capacity

---

- Findings: the general public needs to be well informed to use technology safely; the U.S. needs a technologically advanced workforce.
- Solution: cybersecurity education program for digital safety, ethics, and security; expand and train the cyber workforce
- Approach: increase cybersecurity education; expand Federal IT workforce; promote cybersecurity as an enterprise leadership responsibility



# Shared Responsibility

---

- Findings: the public and private sectors' interests are intertwined; government and industry leaders – both nationally and internationally – need to develop holistic solutions
- Solution: government efficiency; private sector engagement; public-private partnerships and information sharing; shape the international environment
- Approach: government aligning of resources; evaluate barriers to partnerships; integrated approach to policy formulation; coordinate and expand international partnerships



# Incident Response

---

- Findings: need for a comprehensive framework to facilitate coordinated responses by government, private sector, and allies to a significant cyber incident.
- Solution: build a framework for incident response
- Approach: define roles, responsibilities, and resources for Federal departments and agencies; develop thresholds for incident reporting; develop a set of threat scenarios and metrics; implement a National Cybersecurity Center (NCSC); pilot intrusion detection and prevent systems for Federal networks; develop options for information sharing; define private sector roles and responsibilities



# Innovation

---

- Findings: we have a converged platform where data, voice, and video applications share a common infrastructure
- Solution: harness the full benefits of innovation to address cybersecurity concerns
- Approach: develop a coherent and well-conceived architectural concept; create an integrated vision for policies, standards, research, market development, and procurement; provide a framework for research and development strategies that focus on game-changing technologies; establish identity management; maintain national security/emergency preparedness capabilities



# Near-Term Actions

---

- Appoint a cybersecurity policy official
- Prepare an updated national strategy
- Designate cybersecurity as key management priority
- Designate a privacy official to NSC directorate
- Conduct legal analyses and formulate policy guidance
- Initiate public awareness and education campaign
- Develop an international cybersecurity policy framework
- Prepare a cybersecurity incident response plan
- Develop a framework for research and development strategies that focus on game-changing technologies
- Build a cybersecurity-based identity management vision and strategy



# Mid-Term Actions

---

- Expand support for education programs and research and development
- Develop a strategy to expand and train the workforce
- Obtain strategic warning and inform incident response capabilities
- Develop a set of threat scenarios and metrics
- Develop an information sharing process between government and private sector
- Encourage collaboration between academic and industrial labs
- Use the research and development framework to inform standards bodies



# Assessment of White House Strategy

---

- Effort: A
- Research: A
- Style: A-
- Balance: B+
- Substance: B
- Original Thought: C
- Timeliness: D
- Detail: Incomplete



# Themes of Legislative Proposals

---

- Cybersecurity of Federal Government
- Leadership for Cybersecurity
- Protection of Critical Infrastructures
- Identity Theft
- Use of Social Security Numbers
- Regulation of Business
- Security Breach Notifications
- Information Privacy
- Peer-to-Peer Networks



# Regulatory Actions

---

- Department of Education Final Rules for ***Family Educational Rights and Privacy Act***
- Federal Trade Commission Final Rules for ***Notice of Address Discrepancies & Red Flags***
- Federal Communications Commission NOI for ***National Broadband Plan***
- Federal Trade Commission NPR for ***Health Breach Notification Rule***
- Department of Education NPR for ***Higher Education Opportunities Act***



# Higher Ed Opportunities Act

---

## ➤ Peer-to-Peer Filesharing

- An annual disclosure to students describing copyright law and campus policies related to violating copyright law.
- A plan to "effectively combat" copyright abuse on the campus network using "a variety of technology-based deterrents".
- Agreement to "offer alternatives to illegal downloading".

## ➤ Verification of Distance Education Students

- Processes to verify that student who registers in a distance education course is the same student who participates in and complete the program and receives academic credit
- Proposed Regulation: verify identity with a secure login and password or proctored exams; and consider new identification technologies and practices



# Higher Education Information Security Council

---

- formerly EDUCAUSE/Internet2 Security Task Force
- Goals:
  - Obtain Executive Commitment and Action
  - Maintain Data to Enhance Privacy & Security Protections
  - Develop and Promote Effective Practices & Solutions
  - Explore New Tools and Technologies
  - Establish and Promote Information-Sharing Mechanisms
- Initiatives:
  - Student Poster and Video Contest
  - National Cyber Security Awareness Month
  - IT Security Practices Guide



# Campus Safety & Security Project

---

- All-hazards approach to emergency preparedness
- Sponsoring Organizations: NACUBO, EDUCAUSE, IACLEA, CSHEMA, ACPA, AGB, APPA, NACUA, and URMIA
- Phases:
  - Literature Review
  - Survey
  - Campus Site Visits
  - National Conference
  - Final Publication



# Discussion

---

