United States Information and Communications Enhancement Act of 2009

Presentation by Erik Hopkins
Subcommittee on Federal Financial Management,
Government Information, Federal Services,
and International Security

Overview

- Where did FISMA 2002 Leave Us?
  - Strengths and Weaknesses
- What is the State of Global Cyber Space?
- What is the State of Government Information?
- What did “FISMA 2.0” Accomplish
  - Improvements
- Where will US ICE Act of 2009 Take Us?
  - Where Do We Go From Here

FISMA 2002 Strengths

- Increased awareness of senior management
- Dedicated resources to measuring security
- Established effective security policies, procedures, and controls
- Established a framework to assess and balance “risk”

FISMA Raised the Bar

FISMA Weaknesses

- “Governance” structure lacked true accountability
- Agencies lacked needed guidance and direction
- Congress and OMB established a compliance mindset
- Measures of “success” lack effectiveness and results
- Relatively no recognition that systems are interconnected, boundaries change every day, attacks come from new vulnerabilities and exploits
- Little to no guidance for new mediums of technology

FISMA is Holding Us Back

What is the State of Cyber Space?

- Global information infrastructure
  - Predominately private owned
  - Key to Global economic health and productivity
  - Key to democracy and freedom of expression
- The US is the greatest benefactor, yet most at risk
  - US wealth creation predominantly relies on the global information infrastructure
  - Current system allows for asymmetric “warfare”
  - Laws/ Policies/ Social Norms Trail behind

Cyber Space is Key to the Vitality of America
but with the Maturity of a 5 Year Old

What is the State of Gov Information?

- 9/11 showed us that we need effective information sharing (Kinetic attack)
- Recent cyber attacks showed us we need to build better walls (Cyber attack)
- US code and public laws are arcane
- Agencies don’t know what information they hold, who has access, and whether it has been compromised

Need to Balance Information Sharing and Information Security?

What Did “FISMA 2.0” Do?

Interviews 2009

- Tom Davis: “Well I think we are ready to take it to the next stage at this point, but at the time I think it took it to a level where you created an awareness in the department, you created some appropriate awareness within it and some guidelines for them to follow and we followed it up with the grades, and I think as a result of that we made some improvements. That was years ago and I think we are ready now, and we have been ready, to take it to another level.”
- Karen Evans: “Minimizing risk requires agencies to move beyond compliance; which still only represents a starting point in assuring secure data and systems. Compliance alone, as we have learned through painful experiences, will not guarantee information security.”

"FISMA 2.0" Accomplishments

- Established accountability with CISO
  - Budget and Access
- Offense informs defense
  - Limited resources need to be focused
- Recognized interconnected nature of "systems"
  - Broke down artificial boundaries
- Government needs to use purchasing power
  - Public-private partnership to enhance security of COTS

"FISMA 2.0" Updated Government Thinking

Where Will U.S. ICE Take Us?

- Recognized global interconnectedness
- Increased situational awareness
  - Leverage entire Federal government resources
- Greater accountability within agencies
- Enhanced monitoring, detection, and responsive
- Elimination of distinction between NSS/ NNSSS
- Effective partnership between public demand and private supply

Paradigm Shift in Cyber Space

Questions?

erik_hopkins@hsgac.senate.gov