Possible Government-Wide Information Security Enhancements

Some Informal and Unofficial Thoughts

September 2004

Key Topics

- FISMA is a critically important piece of information security legislation, but a sterile evaluation of an agency's security program based on the language of the law alone might not adequately measure and credit enterprise-wide security enhancements.

- For a more practice-oriented evaluation, is it possible to leverage the combined expertise and resources of the Chief Information Officer (CIO) community to identify and proliferate common enterprise-wide security programs, capabilities and tools for CIOs to deploy?

FISMA

- **The current system-by-system, site-by-site approach does not adequately credit agencies for infrastructure security programs**
  - Defense-in-Depth boundary and backbone protections are not sufficiently measured and credited
  - FISMA evaluations may not accurately reflect or give credit for gateway hardening, perimeter defense, telecomm modernization, professionalization of information security workforce, world class incident response and management, enterprise-wide configuration control, …
- **As a result, it's possible for one agency to get a higher annual grade than another agency with overall better infrastructure security**
- **At least one agency's General Counsel has issued an opinion holding that the CIO is given no authority to "enforce" FISMA compliance, only to "ensure" compliance by others who do not have information security qualifications**
- **What can the ISPAB propose to improve this situation?**

FISMA "Extra Credit"

- "Common security controls" are referenced in NIST 800-37, *Guide for the Certification and Accreditation of Federal Information Systems*, as controls that the CIO sponsors on an enterprise-wide basis, with agreement from other senior agency officials, as minimum baseline controls for the agency
- Building on this reference, it may be possible to define "common security technologies, oversight policies and management procedures" that, when implemented by the CIO across an enterprise, greatly increase the security of the enterprise
- Identifying them is the first step; determining how to measure them is also essential

This Concept Extends Beyond FISMA

- Is there an opportunity to leverage the combined expertise and resources of the federal CIO/CISO community to improve security across the government?
- Since information security is critical to government operations, why does each agency have to create and fund its own "one-of-a-kind solution" for every information security program, capability or tool?
- Is it possible to put a government solutions clearing house in place to showcase value-added technology controls, operational controls and management controls to support government-wide programs, capabilities and tools?
- Would such a clearing house achieve efficiencies, economies of scale and overall better information security?
- What would a systematic approach to these enhancements look like?

Current Situation Is Not Efficient

- **Is there an opportunity to create economies of scale?**
  - Centralized department/agency FISMA data collection and reporting database
  - Information security workforce professionalization/certification
  - Government-wide information security Web portal
  - Annual national information security conference
  - Independent technology evaluations
  - Government-wide technology licenses
  - Configuration guides/standards
  - Red teaming, independent testing
  - Identification and proliferation of best practices
- **If these capabilities existed as national resources over the past 4 years, at least one department would have saved about 50% FTE and more than $50 million in creating "one-offs"**
- **There's a real void to be filled, providing government-wide programs, capabilities and tools**

Potential ISPAB Recommendations

- Regarding FISMA …
  - Define infrastructure “common security technologies, oversight policies and management procedures” that the CIO can put in place for the enterprise
  - Define measures for these controls so that “extra credit” can be provided in the annual grades
  - Consider whether or not it makes sense to give CIOs the authority to enforce configuration control
  - Consider whether or not the General Counsel opinion from one agency on the CIO’s lack of authority to enforce (“ensure”) compliance under the law is accurate
- Regarding a cross-government effort …
  - Propose that an entity be established to put in place truly value-added, government-wide programs, capabilities and tools to achieve efficiencies and economies of scale throughout the federal government … *with OMB oversight and enforcement*