IG PCIE Panel on FISMA

Information Security and Privacy Advisory Board

Judy Gordon
Assistant Inspector General for Systems Evaluation
U.S. Department of Commerce
December 7, 2006

Has Commerce Enhanced Security Under FISMA?

- Information Security Is Improving Under FISMA.
  - Our initial independent evaluations found numerous problems:
    - Historically, senior management has given information security little attention and support.
    - Because of this neglect, IT security weaknesses were pervasive and placed sensitive systems at serious risk.

Has Commerce Enhanced Security Under FISMA?

- Initial evaluations found
  - Security plans failed to provide foundation for security control assessment.
  - Security control assessments did little more than scan for vulnerabilities.
  - Few systems received continuous monitoring.
  - Protection of government information in contracts received little attention.

Has Commerce Enhanced Security Under FISMA?

- Since FISMA
  - Senior management gives greater attention to information security.
  - Improvements have followed:
    - Department-wide information security policy and program.
    - Bureau security programs, practices, and controls.
    - Information security in contracts.
    - System certification and accreditation.
- Yet much remains to be done to establish a repeatable process for ensuring an adequate, consistent information security program throughout the Department.

Is C&A Just a Paperwork Exercise?

Is C&A Just a Paperwork Exercise?

- C&A is essential for effective information security, and if done correctly, it
  - Helps ensure system security controls are appropriate and working as intended.
  - Better enables senior management officials to spend IT security dollars on highest priority needs.
- Commerce continues to improve its C&A, but needs to significantly enhance security control assessments.

Systems are certified and accredited though many controls are not assessed . . .

Extract from Finding on Adequacy of Security Control Assessment From Recent OIG C&A Review

	Function	Application Server	DB Server	Domain Controller	Mail	Application Server	Workstations	Application 1	Oracle DB	Router	Firewall
	Operating System	NT	UNIX	W2K	W2K	Linux	XP/W2K				
	Control Name										
AC-2	Account Management			X					X		
AC-3	Access Enforcement				X						
AC-5	Separation of Duties				X		X				
AC-7	Unsuccessful Logon Attempt			X							
AC-8	System Use Notification						X		X		
AC-11	Session Lock						X				
AC-12	Session Termination			X							
AC-17	Remote Access										
AC-19	Access Ctl-Mobile Sys										
IA-2	User ID & Auth				X						
IA-3	Device ID & Auth										
IA-4	Identifier Management								X		
IA-5	Authenticator Management			X					X		
CM-6	Configuration Settings										
RA-5	Vulnerability Scanning	X	X	X			X				X

X Control assessment performed

Potentially required control assessment step was not implemented

Control assessment not applicable

How Do We Approach FISMA Reviews?

- We assign them to highly skilled technical staff.
  - Educational backgrounds and professional experience in computer science and information security.
  - Certifications:
    - Certified Information Systems Security Professional (CISSP)
    - Certification and Accreditation Professional (CAP)
    - Certified Ethical Hacker (CEH)
    - NSA INFOSEC Assessment Methodology (IAM)
    - NSA INFOSEC Evaluation Methodology (IEM)
    - Certified Information Security Manager (CISM)
- We follow PCIE Quality Standards for Inspections.

How Do We Approach FISMA Reviews?

- Our criteria are
  - NIST standards and guidance.
  - OMB guidance.
  - Department of Commerce IT security policy.
- Our focus has been on
  - C&A, especially quality and completeness of security control assessments.
    - Does authorizing official have enough information about remaining vulnerabilities?
  - Secure configuration settings (CM-6).
  - Continuous monitoring.

How Well Does Commerce Follow NIST Standards and Guidance?

- Users continue to wrestle with application of the standards.
- All parties would benefit from a better understanding of NIST framework and associated standards and guidance.
  - Authorizing officials, system owners, certification agents, information security officers, and C&A support contractors.
- Commerce CIO's office has been providing training.
- It would be helpful for NIST to develop examples of required C&A documents.
  - Security plans, risk assessments, security control assessment plans and assessment results.

Is Senior Management On Board With FISMA?

- FISMA is supported by senior management of Department as well as senior bureau management.
- However, authorizing officials and system owners often appear to not understand or accept their responsibilities.

What Progress Has Your Agency Made in Protecting Citizens' Privacy?

- Revising policy to better address privacy requirements.
- Using 30-minute "time-out" policy.
- Encrypting data on mobile devices.
- Preparing solicitation for two-factor authentication.
- Reporting incidents to DHS within one hour.