CACI

EVER VIGILANT

Information Security Metrics

Bruce A. Brody, CISSP, CISM

Vice President, Information Assurance

December 8, 2006

Key Questions

- Is it possible to receive a high FISMA grade and not have a “secure” enterprise?
- Worse, is it possible for an agency with a high FISMA grade to be unaware that its enterprise has been compromised?
- Does FISMA measure the right things?
- If not, what should we be measuring?

Problems with the FISMA Grades….

2005 Grading Categories	2005 Points	What's Missing?
A. Annual Testing	20	Does not specify technical testing on a continuous basis, and does not empower the CIO to conduct it
B. Plans of Action and Milestones	15	"Paperwork" that is not always connected to underlying technical processes
C. Certification and Accreditation	20	It is possible for 100% of systems to receive a valid C&A but not be considered secure
D. Configuration Management	20	Does not require continuous vulnerability management
E. Incident Detection and Response	15	Does not measure whether incidents can be prevented, or what the business impact is
F. Training	10	Measures if training merely was conducted, but does not measure quality or effectiveness of training
G. Inventory	-10	Almost unknowable in a geographically distributed and highly decentralized enterprise

FISMA could be improved by requiring and measuring rigorous technical controls….

For Effective Federal IT Security….

CACI
EVER VIGILANT

The CIO Must Know With 100% Certainty…	Which Requires Technology For…	Which Can Be Measured By…
1. What are the boundaries and the topologies of the interconnected enterprise?	• Network Discovery and Mapping • Network and Enclave Boundary Controls • Boundary Verification and Leak Detection • Wireless Access Scanning • Comm. Encryption (Link/Site-Site/Pt-Pt)	• Can the external boundaries and interconnections and internal boundaries and topology of the enterprise's networks be reliably determined, characterized and understood at any point in time?
2. What are the connected devices and what are the associated communications on the enterprise's networks?	• Device Discovery and Identification • Network Traffic Flow Analysis • Network Traffic Content Analysis • Network Intrusion Detection and Prevention • Network Traffic Filtering and Malware Protection	• Are all of the connected devices known and identified at any point in time? • Are all intercommunications known, authorized and understood? • Can the devices and communications involved in, or potentially affected by, a security incident be readily identified as it is occurring?
3. How are those devices configured?	• Software and Patch Management • Security Settings Management/Hardening • Vulnerability Assessment and Remediation • Host Malware Protection • Host Firewall and Intrusion Prevention • Network Access Control (Verify/Quarantine)	• What are the existing vulnerabilities and potential cascading attack vectors? • Can critical security patches be promptly tested and deployed to all affected devices? • How often are device configurations verified and residual vulnerabilities identified?
4. Who is accessing those devices? - Is the access authenticated / authorized?	• Identity/Access Authorization Management • Strong/Multi-Factor Authentication • Directories and Public Key Infrastructure • Identity Based Network Access Control • Training, Education, Awareness	• What percent of the software, users and suppliers have been reviewed for security? ➢ How long has it been since this review? • Can all system and information access be uniquely tracked to an individual user?
5. What are the authorized (and unauthorized) users doing while accessing those devices?	• Audit – Aggregation and Analysis • Policy Enforcement • Anomaly/Incident Detection, Analysis and Containment • Incident Correlation/Protection/Prevention • Forensics	• Can incidents be detected, analyzed and responded to as they are occurring? • What is the business impact and underlying cost attributable to security incidents? • What was the impact of incidents that were not promptly detected and contained?

Conclusions

- **FISMA is better than nothing, but now is a good time to improve it**
- **FISMA must evolve from largely paper-based compliance processes to technology-based security processes**
- **The soon-to-be Majority Staff of the House Committee on Government Reform has taken intense interest in this issue**

The real bottom line – We must protect our nation's critical information technology infrastructure and resources from those who wish to do them harm!