Information Technology Security Assessment Framework

John Gilligan

Chief Information Officer
Department of Energy

June 13, 2000

Security, Privacy, and Critical Infrastructure Committee

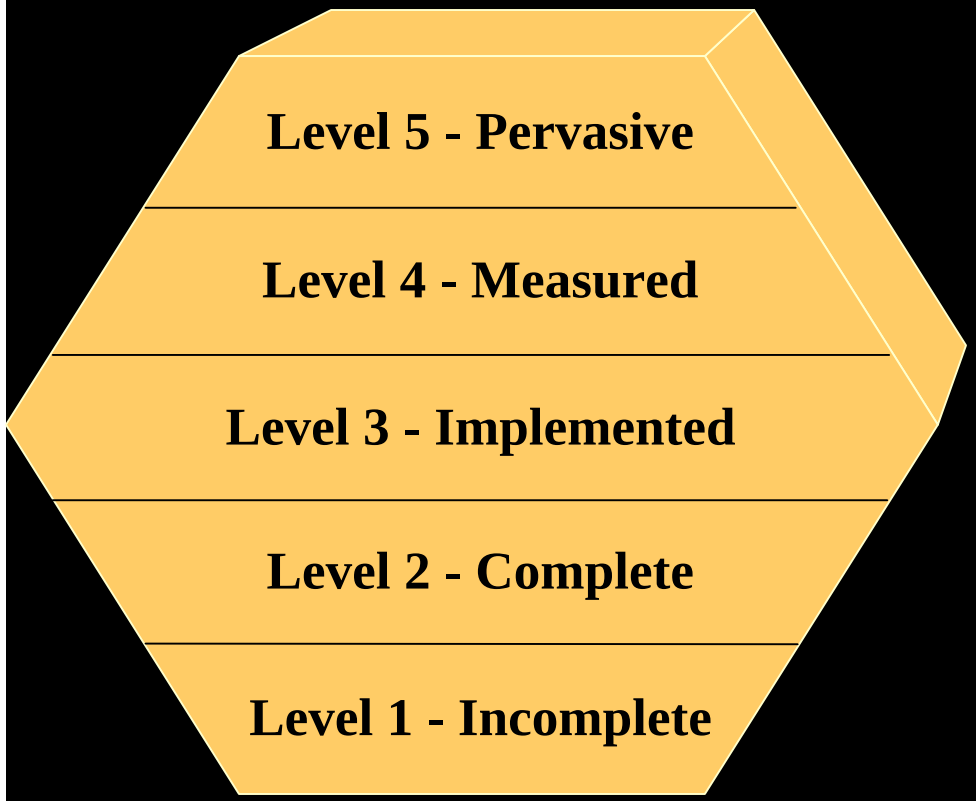
Development of the Information Technology Security Assessment Framework

- Recognized need to improve the security of Federal agencies' information resources and IT systems
- Although we have tools, guidelines, and standards for individual application systems, we lack an effective management level metric for security
- The CIO Council is developing a measurement framework for determining the maturity of an agency's IT security program

Objectives of the Framework

- Provide guidance to Agencies for self measurement of information systems security
- Emphasize priority attention to “foundation” activities
- Provide a guide for evolving to more robust and more effective security
- Support immediate implementation

Framework Description



- Leverages established GAO, OMB, and NIST Guidance (GAO FISCAM, OMB A-130, NIST SP-800-14)
- Provides immediate opportunity for agencies to work toward meeting lower levels while higher levels are being refined

Level 1 - Incomplete

- Documented, but an incomplete security program encompassing most major agency components
- Includes approved system security plans for most general support systems and major applications

Level 2 – Complete

- Well documented, complete security programs that meets all basic requirements of statutory and policy authorities

- Encompasses **all** major agency components and includes system security plans for **all** general support systems and applications

Level 3 - Implemented

- Is well defined and implemented security program with detailed implementation procedures covering level 2 capability
- Has been fully promulgated across all elements of the organization
- Encompasses all major agency components

Level 4 - Measured

- Is a measurable security program
- Has the capability of comparing cost of security features to a resulting decrease in security vulnerabilities
- Assumes the existence of metrics and a process to analyze the metrics so effectiveness can be evaluated

Level 5 - Pervasive

- Is a pervasive, continuously improving security program that applies the level 4 capabilities to increase security program cost-effectiveness
- Is agile, able to respond quickly to changes in threat, system characteristics or organization mission

Future of the Framework

- More granularity of existing criteria and expansion and refinement of levels 4 and 5
- Determining effectiveness of processes
- Measurement of cost-effectiveness
- Development of security checklists to determine what cost-effective activities are being undertaken