# FISMA:
# Facts and Fiction

# What is FISMA?

FISMA (the Federal Information Security Management Act of 2002) is Title III of the Electronic Government Act, passed by the 107th Congress and signed into law by the President in December 2002. FISMA recognized the importance of information security to the economic and national security interests of the United States.

# What is FISMA?

FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

# How does FISMA work?

FISMA, along with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), explicitly emphasizes a risk-based policy for cost-effective security. FISMA, requires executive federal agencies to:

- Plan for security
- Ensure that appropriate officials are assigned security responsibility
- Periodically review the security controls in their information systems
- Authorize system processing prior to operations and, periodically, thereafter

# FISMA Facts

The facts about FISMA:

- 1) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets
- 2) recognizes the highly networked nature of the current Federal computing environment and provide effective Government-wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities
- 3) provides for development and maintenance of minimum controls required to protect Federal information and information systems

# FISMA Facts

- 4) provides a mechanism for improved oversight of Federal agency information security programs
- 5) acknowledges that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector
- 6) recognizes that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products

# FISMA Fiction

Some myths about FISMA:

- 1) FISMA is fundamentally flawed
- 2) Metrics being captured aren't improving security
- 3) C&A and risk assessments are a paperwork exercise
- 4) FISMA compliance diverts critical resources away from implementing information & network security
- 5) FISMA compliance doesn't guarantee a secure system
- 6) There is no one "right" way to conduct FISMA compliance

# Summary

While there may be federal agencies that purposely comply with the letter of FISMA, while simultaneously not improving the security of their systems, the consensus is that most agencies want to and do conduct themselves according to the intended purpose of FISMA: the improvement of system security.

To make the most of FISMA compliance and increased information security, resources must be provided. This will enable the Secret Service to maintain a high degree of protection over its highly sensitive mission-critical information, systems and networks.