Federal Information Security Modernization Act (FISMA)

Protection Mandate
- Mandates safeguarding US Government owned, and operated, systems and data

Digital Era Response
- Recognizes the need for strong security controls due to growing digital government operations

Economic & National Security
- Addresses information security as critical to US economic and national interests

Cybersecurity Focus
- Aims to protect federal government against unauthorized activities and ensure system/data integrity, confidentiality, and availability

- Protection of national security & sensitive data
- Increasing complexity & dependence on Information Technology
- Rising cybersecurity threats
- Need for standardized security practices / controls
- Compliance & accountability

Key Expectations

Risk Management

Focuses on a risk-based approach for cost-effective security

Security Controls

Agencies must meet minimum security requirements

Operationalize (via RMF)

Requires the development of system security package addressing 800-53 control families

Compliance & Reporting

Agencies must implement security best practices & report to Congress

2014 Modernization Updates

Federal Information Security Modernization Act of 2014	• Refined reporting requirements & emphasized cyber breach notification & efficiency in reporting
Leadership Role for Department of Homeland Security (DHS)	• Authorized the Secretary of DHS to assist OMB in administering information security practices for federal systems, including developing “binding operational directives"
Reporting Requirements	• Shifted the focus to threats, security incidents, and compliance with security requirements
Cyber Breach Notification	• Requires Executive Branch civilian agencies to notify & consult with US-CERT regarding information security incidents