MEMO

UNDERSTANDING THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2002

To: Representative Tito Canduit

From: Gavin Williams, Legislative Research Aide

Date: 12/1/2023

Class: CYSE406 – Cyber Law

COMMENTS: This memo provides a comprehensive overview of the Federal Information Security Modernization Act (FISMA) of 2002, a significant U.S. cybersecurity law. It aims to assist in your efforts to communicate the importance of cybersecurity legislation to constituents in the 26th District of Virginia.

Overview

The Federal Information Security Modernization Act (FISMA), passed in 2002, plays a important role in how the U.S. government handles cybersecurity. This law tells federal agencies that they must put in place certain security measures to keep their computer systems and data safe. The goal is to ensure that all the sensitive information these agencies have is kept confidential, free from any unauthorized alterations, and always available when needed. To do this, FISMA requires agencies to regularly check their security measures, test them, plan for potential cyber incidents, and keep an eye on their security setups at all times. Additionally, these agencies have to regularly show that they are following FISMA's rules to both the Office of Management and Budget and the Department of Homeland Security.

History

In the late 1990s and early 2000s, there was a large increase in cyber threats and major security incidents. This made it clear that the U.S. government needed a better, more unified way to protect its computer systems and data. Thus, FISMA was created. FISMA required every federal agency to set up a detailed program for keeping their information and systems secure. This program needed to cover all aspects of security, not just for their own systems but also for any systems managed by other agencies, contractors, or any outside sources.

Problems Addressed by the Legislation

The Federal Information Security Modernization Act (FISMA) addresses several key problems in the realm of government cybersecurity:

- **Lack of Standardized Cybersecurity Practices**: Before FISMA, there was no uniform approach to securing federal information systems, leading to inconsistent security levels across different agencies.
- **Vulnerability to Cyber Threats**: FISMA provides a framework to protect government data and infrastructure from cyberattacks, reducing vulnerability to these threats.
- **Insufficient Risk Management**: The act requires regular risk assessments, ensuring that agencies continuously evaluate and manage potential security risks.
- **Inadequate Incident Response**: FISMA requires agencies to have formal incident response plans, improving preparedness and response to cybersecurity incidents.
- **Lack of Accountability**: By requiring agencies to report their compliance to the Office of Management and Budget and the Department of Homeland Security, FISMA ensures agency accountability by them having to implement effective cybersecurity measures.

While FISMA has its strengths, it also faces several challenges:

- **Difficulty Sharing Information:** Difficulty in sharing cybersecurity information across different agencies.
- **Needs Continued Compliance:** The need for continuous updates to FISMA to address new cyber threats.

- **Security Planning Focus:** FISMA focuses more on the process of security planning rather than the actual effectiveness of the security measures.
- **Complex:** The possibility of confusion due to the complexity of controls outlined by FISMA.
- **Baseline not Endpoint Measures:** FISMA should be viewed as a foundational guideline for security measures, not the comprehensive endpoint.

In summary, FISMA solves important issues related to cybersecurity management and response for federal agencies, thus increasing the overall security of government information systems.

Effectiveness

FISMA has significantly enhanced the ability of federal agencies to manage their cybersecurity by providing a framework for protecting information. This framework has established clear guidelines for maintaining information security. However, in today's world where technological advancements and cyber threats are increasing rapidly, there is a pressing need for FISMA to be regularly updated. Adjustments that allow FISMA to effectively address new technologies and threats, combined with increased collaboration with private sector cybersecurity specialists, would increase its usefulness. Continuous improvement of FISMA is necessary to ensure it stays an effective tool against new cyber risks.

Voter Relevance

Voters should care about FISMA because it directly impacts the security of their personal data held by federal agencies. As more services move online, from tax filing to health benefits, the protection of this data becomes crucial. FISMA's role in protecting government information systems against cyber threats is necessary to ensure that sensitive personal information does not fall into the wrong hands, thus maintaining public trust in government operations. Additionally, in an era where national security is increasingly connected to cyber security, FISMA's effectiveness is crucial in protecting the nation's critical infrastructure, which then supports the overall well-being and security of its citizens.

[see references on next page]

References

Chief Information Officers Council. (n.d.). Federal Information Security Modernization Act (FISMA). CIO.gov. Retrieved 11/30/2023, from https://www.cio.gov/handbook/it-laws/fisma/

Gillis, A. (2020, September 22). *What is FISMA (Federal Information Security Management Act)?*. Security. https://www.techtarget.com/searchsecurity/definition/Federal-Information-Security-Management-Act

IT Governance USA. (n.d.). Federal Information Security Management Act of 2002 (FISMA). Retrieved [insert retrieval date], from https://www.itgovernanceusa.com/fisma