Nathan Cosendine
Policy Analysis Paper 1
CYSE425W
1/28/2024

The Federal Information Security Management Act

The Federal Information Security Management Act or FISMA was first created as part of the E-Government Act of 2002, but was later amended in 2014. FISMA is a cybersecurity policy designed to ensure that security programs within the federal executive branch agencies stay under a certain risk level. This policy tasks the Department of Homeland Security (DHS) with the responsibility of developing and overseeing the implementation of information security policies. Federal government agencies are accountable for adhering to these standards in order to be deemed FISMA compliant. Another aspect of FISMA of 2014 is the reestablishment of oversight authority to the Director of the Office of Management and Budget (OMB). Through this act, the OMB is responsible for determining what a major incident is, as well as assessing the efficiency of implemented information security protocols.

In order to be qualified as FISMA compliant, federal agencies must meet specific qualifications and take certain actions. This includes things like conducting risk assessments, categorizing information systems based on risk level and importance, performing annual security reviews, implementing continuous monitoring, adhering to baseline security controls, and documenting these controls in a system security plan.

Agency security reports are to be created yearly and given to Congress, DHS, and OMB. These annual reports include the detailing of any major incidents, threats, vulnerabilities, and incident numbers. Categorizing information systems based on risk level and importance is crucial part of the security program. Agencies should classifying systems in order to determine which information and systems pose of the highest risk and require the highest level of security.

Continuous monitoring is vital for agencies to quickly catch any breaches or attacks on their information systems. Constant monitoring also means consistently looking for any potential weaknesses in their systems. Failure for federal agencies to be FISMA compliant will result in penalties ranging from a less government funding to a formal statement of disapproval from congress.

I chose this particular policy as it plays a vital role in shaping cybersecurity practices within the federal government. By establishing an extensive security standard, FISMA ensures consistency across federal agencies, providing a framework that guarantees the security of federal information. This baseline standard increases the security of federal information both at the federal and state level agencies. This baseline is also important for businesses in the private sector, as they now have government approved security policies they can adhere to.

In summary, The Federal Information Security Management Act is an essential component of government cybersecurity rules and regulations. Its creation came in response to the pressing requirement that federal agencies have a uniform strategy for information security. As technology advances, it comes with an increase in security threats. It is important that the United States government stay ahead in the cyber security field in order to protect its citizens and upkeep national security.

Works Cited

CMS Information Security & Privacy Group. (n.d.). https://security.cms.gov/learn/federal-information-security-management-act-fisma

Federal Information Security Modernization Act: CISA. Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act

Lord, N. (2023, May 6). *What is FISMA compliance? (definition, requirements, penalties, & more)*. Digital Guardian. https://www.digitalguardian.com/blog/what-fisma-compliance-fisma-definition-requirements-penalties-and-more

S.2521 - 113th congress (2013-2014): Federal Information Security ... congress. (n.d.). https://www.congress.gov/bill/113th-congress/senate-bill/2521