Discussion post

Name

Professor

Institutional Affiliations

Course

Date

Discussion post 2

According to my research this is what I found on FISMA reports:

FISMA stands for the Federal Information Security Modernization Act, which is a United States law that requires federal agencies to implement information security programs to protect their data and systems. As part of this law, federal agencies are also required to submit annual reports on the state of their information security programs, known as FISMA reports.

These reports are meant to provide an overview of the agency's information security posture, including any vulnerabilities or weaknesses that have been identified, as well as the steps the agency is taking to address these issues. The reports are used by Congress and other oversight bodies to evaluate the effectiveness of federal agencies' information security programs and to identify areas where additional resources or attention may be needed

The FISMA reporting process involves several steps. First, the agency must conduct a comprehensive evaluation of its information security program, using a set of guidelines established by the National Institute of Standards and Technology (NIST). This evaluation includes an assessment of the agency's risk management practices, security controls, and incident response capabilities, among other things.

Once this evaluation is complete, the agency must submit a FISMA report to Congress, the Office of Management and Budget (OMB), and the Department of Homeland Security (DHS). The report must include a description of the agency's information security program, an assessment of the program's effectiveness, and a summary of any security incidents or breaches that have occurred over the past year.

The FISMA reporting process is an important tool for ensuring the security of federal information systems. By requiring agencies to regularly evaluate their security programs and report on their progress, FISMA helps to identify areas where additional resources or attention may be needed, and promotes a culture of continuous improvement in information security

. In conclusion, FISMA reports are annual reports submitted by federal agencies to provide an overview of their information security programs and any vulnerabilities or weaknesses that have been identified. These reports are an important tool for evaluating the effectiveness of federal agencies' information security programs and identifying areas where additional resources or attention may be needed.

References:

- "Federal Information Security Modernization Act of 2014," Pub. L. No. 113-283, 128 Stat. 3073 (2014).

- National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," SP 800-30 Rev. 1 (2012).

- U.S. Government Accountability Office, "Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs," GAO-21-467T (2021).