What is a FISMA Report?

Definition of FISMA

**FISMA** stands for the Federal Information Security Management Act. It is a United States (U.S.) federal law passed in 2002 that seeks to establish guidelines and cybersecurity standards for government tech infrastructure, and in so doing protect government information and operations. FISMA defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats.

A **FISMA report** is a document that summarizes the implementation and effectiveness of the Federal Information Security Modernization Act of 2014 (FISMA) by federal agencies. FISMA is a law that requires federal agencies to develop, document, and implement an information security and privacy program that protects their information and information systems from unauthorized access, use, disclosure, modification, or destruction.

**A FISMA report typically consists of three main sections:**

# CIO Section

This section reports on the implementation of FISMA cybersecurity assessment and performance (CAP) measures and base measures by the agency’s Chief Information Officer (CIO). These measures evaluate the agency’s cybersecurity posture, maturity, and capabilities across various domains, such as identity management, data protection, incident response, risk management, and governance. The CIO section should include the following elements:

* Data tables, charts, graphs, narratives, and evidence to support the FISMA CAP measures and base measures, such as the percentage of systems with valid authorities to operate (ATOs), the percentage of systems with continuous monitoring capabilities, the percentage of users with strong authentication credentials, the number and severity of cybersecurity incidents, the number and status of Plans of Action and Milestones (POA&Ms), and the level of maturity for each domain.
* A description of the agency’s information security program, including its policies, procedures, standards, guidelines, roles, responsibilities, resources, training, awareness, and reporting mechanisms.
* A description of the agency’s information security strategy, including its goals, objectives, priorities, initiatives, challenges, risks, opportunities, and alignment with the agency’s mission and strategic plan.
* A description of the agency’s information security performance, including its achievements, outcomes, impacts, gaps, weaknesses, lessons learned, best practices, and recommendations for improvement.
* A description of the agency’s information security governance, including its organizational structure, decision-making processes, oversight mechanisms, stakeholder engagement, coordination with other agencies or entities, and compliance with laws and regulations.

## SAOP Section

The SAOP section of a FISMA report is a detailed report on the implementation of a privacy program in compliance with the Privacy Act by the agency’s *Senior Agency Official for Privacy* (SAOP). This section covers the agency’s privacy policies, procedures, training, assessments, breach response, and oversight activities. The SAOP section should include the following elements:

* Data tables, charts, graphs, narratives, and evidence to support the privacy program activities, such as the number and type of *Privacy Impact Assessments* (PIAs), *System of Records Notices* (SORNs), *Privacy Act Statements* (PASs), privacy training sessions, privacy complaints, privacy breaches, and privacy audits or reviews.
* A description of the agency’s privacy program, including its policies, procedures, standards, guidelines, roles, responsibilities, resources, training, awareness, and reporting mechanisms.
* A description of the agency’s privacy strategy, including its goals, objectives, priorities, initiatives, challenges, risks, opportunities, and alignment with the agency’s mission and strategic plan.
* A description of the agency’s privacy performance, including its achievements, outcomes, impacts, gaps, weaknesses, lessons learned, best practices, and recommendations for improvement.
* A description of the agency’s privacy governance, including its organizational structure, decision-making processes, oversight mechanisms, stakeholder engagement, coordination with other agencies or entities, and compliance with laws and regulations.

### IG Section

The **IG** section of a FISMA report is a detailed report on the independent assessment of the security and privacy programs by the agency’s *Inspector General* (IG). This section contains questions about the security and privacy programs independently answered by the IG. These questions assess the agency’s compliance with FISMA requirements, standards, and guidelines, as well as the effectiveness of its security and privacy controls. The IG section should include the following elements:

* Data tables, charts, graphs, narratives, and evidence to support the IG’s answers to the questions, such as the scope, methodology, criteria, findings, conclusions, and recommendations of the IG’s audit or evaluation.
* A description of the IG’s role, authority, independence, and coordination with other oversight bodies or entities in conducting the assessment of the security and privacy programs.
* A description of the IG’s assessment approach, including its objectives, scope, methodology, criteria, sampling, testing, validation, verification, and reporting procedures.
* A description of the IG’s assessment results, including its findings, conclusions, recommendations, and ratings for each question or domain.
* A description of the IG’s follow-up activities, including its monitoring, tracking, reporting, and verifying of the agency’s corrective actions or implementation plans to address the IG’s recommendations.

Submitting a FISMA Report

FISMA report submission is the process of reporting on the implementation of information security and privacy programs in compliance with the Federal Information Security Modernization Act of 2014. FISMA requires agencies to submit annual reports to the *Office of Management and Budget* (OMB), the Congress, and other stakeholders.

The OMB provides agencies with Fiscal Year (FY) reporting guidance and deadlines in accordance with FISMA. The latest guidance is for FY 2023 and was issued on December 2, 2022. The guidance outlines the reporting requirements for the Chief Information Officer, the Senior Agency Official for Privacy, and the Inspector General of each agency.

 The FISMA data is assessed both quarterly and annually. Quarterly, agencies are required to collect FISMA performance metrics data and upload the results into CyberScope. Annually, agencies are required to submit a comprehensive FISMA report that includes the sections from the CIO, SAOP, and IG, as well as a FISMA self-assessment. The annual report is due by October 31 of each year.

Best practices for FISMA reporting

Some of the best practices for FISMA reporting:

* Implement a comprehensive data security plan to classify data, monitor activity, and detect threats to your sensitive data.
* Stay current with any changes to the FISMA standards and guidance.
* Keep documentation of your FISMA compliance efforts and evidence of your security controls.
* Encrypt everything: data encryption is a FISMA requirement.
* Run periodic risk assessments to identify, prioritize and remediate information security gaps.
* Submit your FISMA metrics into the DHS CyberScope application by October 31, 2020, following the instructions in the OMB Memorandum M-20-04.

**Challenges of FISMA Reports**

 Some of the challenges of FISMA reports are:

* Meeting the deadlines and requirements of the OMB and DHS for submitting the FISMA metrics and annual reports.
* Achieving an effective level of security maturity across all domains and functions, as measured by the FISMA metrics ratings.
* Addressing the new security challenges and risks posed by the pandemic, such as remote work, increased cyberattacks, and new applications and systems.
* Implementing and documenting the security controls and processes in accordance with the NIST standards and guidelines.
* Coordinating and collaborating with the agency management, CIO, SAOP, IG, and external auditors to ensure consistent and accurate reporting.

**How to conduct a FISMA report**

 To conduct a FISMA report, you need to follow the guidance and requirements issued by the OMB and DHS, as well as the standards and guidelines issued by the NIST. The process can be divided into six steps:

* **Categorize/Create an Inventory of Information Systems:** Identify and classify your information systems according to their impact level and security objectives, and maintain a comprehensive and accurate inventory of them, including cloud systems, public facing websites, and third-party systems.
* **Select applicable security controls:** Choose the appropriate security controls for your information systems based on the NIST SP 800-53 framework, and tailor them to your specific needs and risks.
* **Implement the security controls:** Apply the selected security controls to your information systems and document how they are implemented.
* **Assess the security controls:** Test and evaluate the effectiveness of your security controls using the NIST SP 800-53A methodology, and identify any weaknesses or gaps that need to be addressed.
* **Authorize the information systems:** Review the results of the security control assessment and make a risk-based decision on whether to authorize the operation of your information systems or not.
* **Monitor the security controls:** Continuously monitor the performance and status of your security controls, and report any changes or incidents that may affect their effectiveness.

**Advantages of FISMA reports**

Some of the advantages of FISMA reports are:

* They help agencies to improve their security posture across the five functions of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover.
* They help agencies to identify and prioritize areas for improvement based on a maturity model that assesses the effectiveness of their security practices.
* They help agencies to comply with federal laws and regulations that mandate information security and privacy programs and practices.
* They help agencies to demonstrate their security capabilities to other stakeholders, such as Congress, OMB, GAO, and potential partners or customers.
* They help agencies to prevent or mitigate data breaches by providing information about the vulnerability of their technology and any potential risks due to human error.

References

Comparitech (January 25,2022) [FISMA Compliance Checklist (comparitech.com)](https://www.comparitech.com/data-privacy-management/fisma-compliance-checklist/)

Chief Information Officer Council [7.4 FISMA Reporting | CIO.GOV](https://www.cio.gov/handbook/reporting/fisma-reporting/)

Cybersecurity & Infrastructure Security Agency [FY 2022 Core IG FISMA Metrics Evaluation Guide](https://www.cisa.gov/sites/default/files/publications/FY%202022%20Core%20IG%20FISMA%20Metrics%20Evaluation%20Guide%20%2805-12-22%29.pdf)