Anita Chidera Duanne Eluwa
10th April 2021
Cybersecurity Risk Management

Rethinking FISMA and Federal Information Security Policy

FISMA stands for Federal Information Security Management Act of 2002. The advancement and proliferation of information technology (IT) has been hugely beneficial for the federal government [1]. This paper proposes a solution to improve the information security safety measures of the federal government's assets. This will also assist in maintaining the integrity of data and prevents hackers from gaining unauthorized access to classified information. The vast majority of federal agencies are delinquent in meeting their statutory information security obligations [2]. This negligence has however led to the various instances of compromised federal information. To amend the legislative scheme, this research is divided into four (4) parts. The first part talks about the surveys of FISMA's most recent ways of resolving this issue. The second part explores two case studies of agency efforts to implement FISMA and explains how those efforts have fallen short [3]. The third part explains why agencies have failed in these efforts while the last part proposes ways the to improve these drawbacks.

FISMA requires that each agency shall develop and implement an agency-wide information security program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency or other source [4]. FISMA also informs the agencies to develop strategies to prevent their systems from unauthorized access. Once this is done, the agencies then test and evaluate the information system controls to ensure that they are implemented accurately. The compliance with the FISMA legislative scheme has however been slow in compliance which leads us to the second part of this research. A couple of surveys were carried out and one quarter of the surveyed agencies acknowledged serious systemic deficiencies in their FISMA plan of action [5]. The application of the FISMA's processes can sometimes be ambiguous and there are no mechanisms put in place to clarify the ambiguities. This then leads to an inefficient response in the FISMA's results when they are implemented. In the third section, we will review why agencies have failed in these efforts. Unfunded mandate, Unglamorous work, A disinterested public, and a Deficit of accountability and oversight. These are the four (4) major reasons why the agencies have failed in the successful implementation of FISMA. FISMA does not directly bring new funding to the agencies [6]. So, while agencies must perform more work, they must effectively do so within the constraints of their preexisting budgets [7]. Most workers view the FISMA work as something that must be done rather than what they like. This makes them reluctant in their performance. The lack of public interest in FISMA compliance can create complacency within Congress as well [8]. This lack of interest

affects the legislative involvement in security. If the agencies do not implement the FISMA scheme, there is no accountability or punishment from the government, and this leads to the lackadaisical attitude of the workers in performing their tasks. In this last section, we will review the proposed solutions to the failures mention above. The first solution is to coordinate from the top. To ensure agency compliance with FISMA, Congress should amend FISMA to create a position within OMB to oversee all federal information security planning [9]. The second solution is that new incentives should be introduced to induce the FISMA compliance. The third solution is that impromptu inspections should be done regularly to monitor the compliance of the workers. The fourth solution talks proposes that the congress should amend FISMA so that when multiple agencies utilize a single information system, OMB determines which of them bears responsibility for FISMA implementation [10]. And lastly, the last solution proposed is that FISMA should contract private-sector workers to initiate appraisals and incentives. In conclusion, we need to confront these realities quickly and effectively, Congress can finish the task it started and move us closer to a government in which all federal data is secure [11].

References

[1] S. Robert, "Rethinking FISMA and Federal Information Security Policy.," *NYUL Rev*, vol. 81, p. 1844, 2006.

[2] S. Robert, "Rethinking FISMA and Federal Information Security Policy.," *NYUL Rev*, vol. 81, p. 1844, 2006.

[3] S. Robert, "Rethinking FISMA and Federal Information Security Policy.," *NYUL Rev*, vol. 81, p. 1844, 2006.

[4] S. Robert, "Rethinking FISMA and Federal Information Security Policy.," *NYUL Rev*, vol. 81, p. 1844, 2006.

[5] S. Robert, "Rethinking FISMA and Federal Information Security Policy.," *NYUL Rev*, vol. 81, p. 1844, 2006.

[6] S. Robert, "Rethinking FISMA and Federal Information Security Policy," *NYUL Rev*, vol. 81, p. 1844, 2006.

[7] S. Robert, "Rethinking FISMA and Federal Information Security Policy.," *NYUL Rev*, vol. 81, p. 1844, 2006.

[8] S. Robert, "Rethinking FISMA and Federal Information Security Policy.," *NYUL Rev*, vol. 81, p. 1844, 2006.

[9] S. Robert, "Rethinking FISMA and Federal Information Security Policy.," *NYUL Rev*, vol. 81, p. 1844, 2006.

[10] S. Robert, "Rethinking FISMA and Federal Information Security Policy.," *NYUL Rev*, vol. 81, p. 1844, 2006.

[11] S. Robert, "Rethinking FISMA and Federal Information Security Policy.," *NYUL Rev*, vol. 81, p. 1844, 2006.