Name: Emma Humphreys
Date: November 19th, 2023
Class: CYSE 425W
Professor: Malik Gladden
Policy Paper 4: Federal Information Security Management Act (FISMA)

In the dynamic landscape of the digital age, where the interconnectedness of our world is both a boon and a potential vulnerability, the Federal Information Security Management Act (FISMA) stands as a crucial pillar safeguarding the integrity of government information systems. Enacted in 2002 and subsequently amended in 2014, FISMA emerged as a response to the escalating cyber threats that accompanied the rapid proliferation of digital technologies. However, beyond its technicalities and legal frameworks, FISMA is not just a cybersecurity policy; it reflects the intricate interplay between societal forces, political dynamics, and the evolving cultural fabric. FISMA is not merely a product of technical exigency but a manifestation of the societal ethos of its time.

The implementation of the Federal Information Security Management Act (FISMA) has ushered in a series of profound social consequences that extend across various spheres of society. As Trautman notes in his article,

> "All too often cyber defense is view through any of several myopic lenses… However, contemporary cyber security requires a systemic engineering approach that recognizes the organization, cultural and social psychological barriers to effectively dealing with this problem " (Trautman, p.4)

Prior to 2002—when FISMA was adopted—information security was a novel concept and was not considered to be a matter of national security. Until the increase in cyber-attacks on government servers, which forced Congress to establish FISMA 2002 that the US government began to take information security seriously. Within the realm of government operations, FISMA has catalyzed a transformation in how information security practices are perceived and prioritized. The strengthening of federal cybersecurity measures not only reflects an enhanced

commitment to protecting sensitive data but also underscores a shift in the broader societal understanding of the importance of digital security in the public sector.

Simultaneously, in the private sector and critical infrastructure, the compliance requirements imposed by FISMA have triggered a reevaluation of cybersecurity strategies within businesses. This has led to a confluence of economic implications and adaptations within industries, with a need for balance between security mandates and the operational needs of businesses. As noted in the *Regulatory Theory and Applications* chapter titled "The Governance of Cyberspace":

> "Moreover, existing hydra-headed reporting systems might also discourage reporting… some industries are required to report incidents to as many as five competent authorities within a timeframe. They would prefer not to disclose the incident to avoid additional work at the very time they are busy fixing the problem" (Drahos et al., p. 541)

Though initial iterations of FISMA were criticized for being cumbersome in its reporting practices—and some would argue still is—it illuminates the importance of finding the right balance of oversight, and the need for business to continue. When a cyber-event occurs, professionals must focus their attention on the vulnerabilities within the system—and have little time for extra paperwork. However, documentation is needed to illustrate how the intrusion occurred and the steps taken to remedy to prevent further exploits.

Embedded within the legislative framework of FISMA are subtle yet profound echoes of cultural and subcultural dynamics that have shaped its evolution. Cultural perspectives on security, reflecting societal values and attitudes towards privacy, have played a pivotal role in influencing the contours of FISMA. The policy, in many ways, mirrors the prevailing ethos of its time, with considerations of trust, transparency, and individual rights woven into its fabric.

Moreover, within the cybersecurity community, FISMA has been subject to the influences of various subcultures. Von Solm discusses the importance of security culture through his 'waves models'. Von Solm's second wave "The management wave was characterized by security policies, Chief Information Security Officers, organizational structures for IS security and so on" (Rao, p. 6). The policies set-forth by the National Institute of Standards and Technology (NIST) as directed by FISMA encourages the progress of socializing the necessity of cyber-security. The clash and collaboration of subcultural forces within the cybersecurity domain have contributed to the nuanced and evolving nature of FISMA, reflecting the intricate tapestry of values and ideologies that shape our collective approach to cybersecurity in the 21st century.

References:

Drahos, P., Chang, L. Y., & Grabosky, P. (2017). The Governance of CyberspaceL. In *Regulatory theory: Foundations and applications* (pp. 533–551). essay, ANU Press.

Rao, V. S., Ramachandran, S., & Walz, D. (2013). *Information Security Subcultures of Professional Groups in Organizations: A Conceptual Framework*.

Trautman, L. J. (2017). Governing risk and the information silo problem: Engineering a systemic cultural and communications solution for Cyber. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2925352