January 10, 2022

Statement for the Record by
SecurityScorecard
Before the House Committee on Oversight and Reform hearing titled,
"Cybersecurity for the New Frontier: Reforming the Federal Information Security Management Act"

Chairwoman Maloney, Ranking Member Comer, thank you for the opportunity to present SecurityScorecard's testimony related to Federal Information Security Management Act (FISMA) reform.

The dynamic cybersecurity threats facing Federal information systems, laid bare this past year by a series of major incidents, a seismic cyber espionage campaign, and many new vulnerabilities have profoundly affected the Federal information security landscape. To respond, the Federal Government needs to improve its information security risk management policies and keep pace with the dynamic threats to Federal networks and supply chains.

FISMA 2021

On October 2, 2021, the Senate Homeland Security and Governmental Affairs Committee (HSGAC) unanimously passed the Federal Information Security Modernization Act (FISMA) of 2021 (S.2902; FISMA 2021).[1] This bill strengthens cybersecurity across the federal government and improves how agencies, CISA, and OMB collaborate on Federal network cyber incident reporting. SecurityScorecard applauds Congress's bipartisan leadership on FISMA reform, and extends our sincere thanks to you both, as the Committee further examines the FISMA authorities. We also look forward to working with the Committee, and Congress, on manifesting critical FISMA reforms that will improve the Federal Government's capability to monitor, assess, and secure its cyber ecosystem.

[1] https://www.congress.gov/bill/117th-congress/senate-bill/2902?s=1&r=20

FISMA 2021 has the potential to address two key weaknesses of the existing FISMA law. The existing law that agencies must follow only uses qualitative measures to trigger Federal action and employs static reporting to demonstrate the health of Federal IT systems. With the emergence of new technologies and real-time monitoring capabilities, FISMA 2021 should: (1) quantify the effects of significant cyber incidents; and (2) monitor systems continuously in real-time.

Leading up to FISMA 2021

The SolarWinds cyber espionage attack and breach focused media headlines and policy discussions on information security practices. The cyber attack affected thousands of private companies and at least nine federal agencies. In January 2021, Congress held several hearings with SolarWinds executives and other technology company leaders. All of these discussions culminated with the May 2021 Executive Order 14028, “Executive Order on Improving the Nation’s Cybersecurity” (EO), which included several ambitious deadlines to strengthen the cybersecurity of Federal Information Technology (IT) networks.

The proposed legislative update to FISMA is an important first step toward solving supply chain security problems exposed by SolarWinds rather than simply identifying them.

Quantify Significant Cyber Incidents

As part of the EO and existing FISMA statute, Federal Civilian Executive Branch (FCEB) agencies are required to report significant breaches. However, no current standard exists to quantify a “significant cyber incident.”

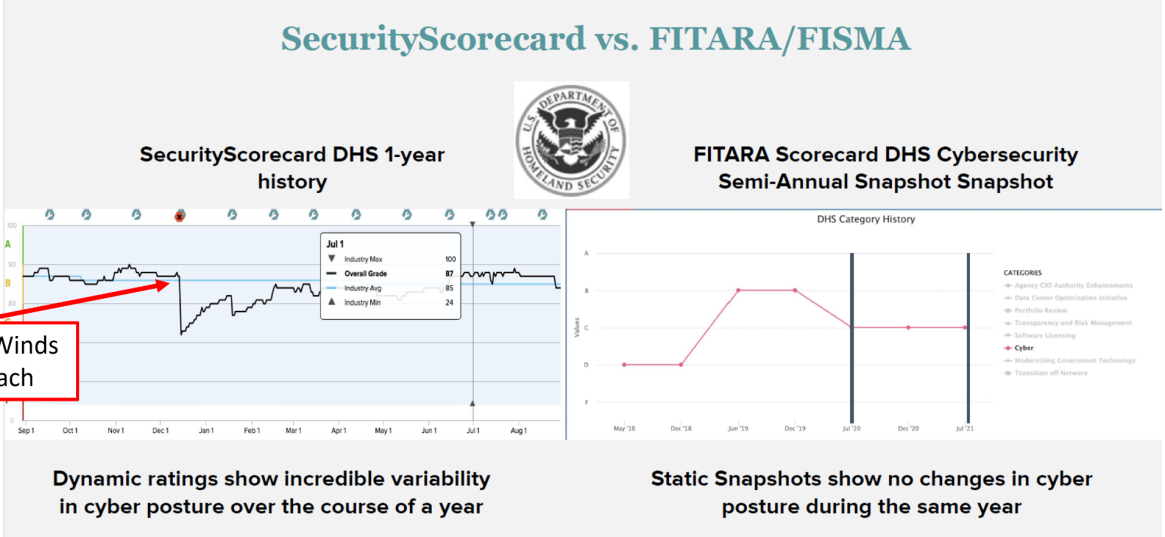
According to news reports, only nine federal agencies were directly breached as part of the SolarWinds attack. Malicious cyber adversaries used administrative privileges to gain complete systems access within Federal networks. The affected nine agencies reported this as a significant cyber incident. Given the highly interconnected nature of agency networks, and the ubiquitous use of SolarWinds in Federal systems, it follows that more agencies might have considered this a significant cyber incident, if only from the perspective of a supply chain attack.

Instead of leaving the definition of a significant cyber incident solely to subjective assessment, and a qualitative judgment, agencies should be identifying incidents with quantitative, statistical measurements. Technology available today can meet this problem quickly and objectively.

SecurityScorecard vs. FITARA/FISMA

Traditionally, the Federal government relies on the FITARA/FISMA score to determine an agency's cybersecurity posture. This presents a point-in-time snapshot that may not adequately reflect continuous changes arising from evolving threats.

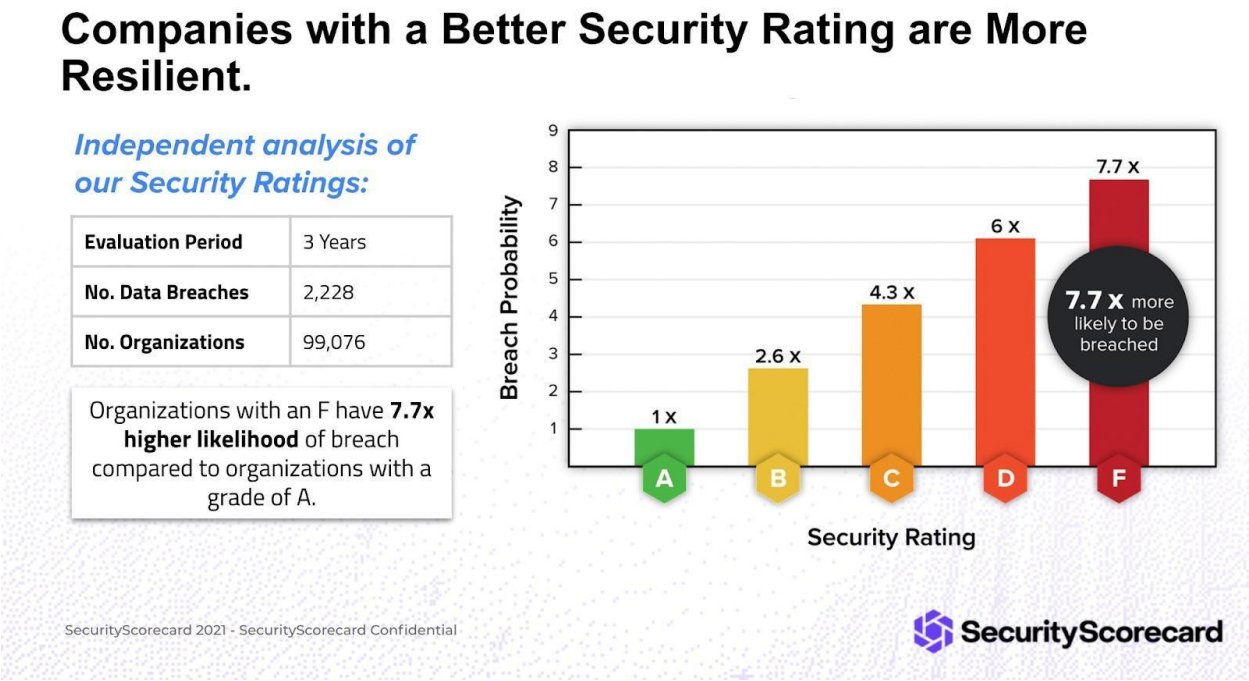
On December 8, 2020, prior to the announcement that Federal networks had been infiltrated by sophisticated nation-state actors, the Department of Homeland Security (DHS) earned a FITARA/FISMA score of 'C.'[2] The most recent FITARA/FISMA score, released in July 2021, also assigns DHS a score of 'C.'[3] Based on these quarterly reports, DHS maintained a stable security posture. However, a look at the historic data available in the SecurityScorecard security ratings platform tells a more nuanced story.



The image above shows the changes in DHS security posture immediately before, during, and for the eight months following the SolarWinds attack announcements.

While the FITARA/FISMA score indicates relative stability over the year, SecurityScorecard's data shows statistically significant volatility. In mid-December, after the SolarWinds announcement, the DHS score dropped 15 points and a full letter grade, from a 'B' to a 'C.' This data shows, according to our advance regression analysis, that the day after the SolarWinds announcement, DHS was twice as likely to be exposed to a cyber or ransomware attack than it was the day before.

[2] https://fitara.meritalk.com/assets/pdf/scorecard-11-methodology.pdf
[3] https://www.fedscoop.com/wp-content/uploads/2021/07/Screen-Shot-2021-07-28-at-2.10.13-PM.png



According to SecurityScorecard's research, agencies with a 'B' score are almost twice as likely to experience a cyber incident than those with a 'C' score. Fundamentally, the research indicates that in the period directly after the SolarWinds attack, DHS's cybersecurity risk nearly doubled. The FITARA/FISMA score gives no visibility into this change. In fact, the static FITARA/FISMA score indicates that DHS had the same level of risk at each of the two reporting points.

Seven months later, DHS had recovered to its pre-SolarWinds posture. However, policy leaders who conduct oversight relying solely on the FITARA/FISMA scorecard would lack visibility into the change in posture and risk.

This indicates a significant gap as policy leaders and agencies look to improve the nation's cybersecurity. Risk continuously evolves, and point-in-time reports lack the real-time quantification necessary to detect and define significant cyber incidents.

Under the FISMA updates, agencies need to gain greater visibility of potential threats. As evident by the differences between the FITARA/FISMA score and SecurityScorecard security rating, agency security posture is a constantly moving target. Further, when a significant cyber incident occurs, agencies may lack visibility into the impact it has on their cybersecurity risk with implications for supply chain attack risks should threat actors move across interconnected federal networks.

The Need for Quantifiable Metrics

Leveraging quantifiable metrics, like security ratings, as part of the definition and reporting of significant cyber incidents, would enhance Federal network security, improve oversight, and build constituent trust. Congress should add quantifiable metrics (and "outside-in," objective data analysis) to FISMA 2021 reform and direct the Office of Budget and Management (OMB) to engage in rule-making to improve the health of the Federal IT ecosystem.

Supply Chain Threats

The highly interconnected nature of Federal networks creates a governmental supply chain issue. An advanced persistent attack (APT) against a single Federal agency that leverages administrative privileges and lateral movement can lead to the compromise of multiple agencies.

Adding quantifiable measures that address this supply chain risk and provide visibility into potential threats affecting all Federal networks. Gaining visibility into how one threat impacts all agencies' security can lead to:

- Enterprise-wide increases in the cyber health of Federal networks;
- Regulation clarification;
- Increased public trust in Federal IT systems; and
- Enhanced oversight capabilities for Congress, the White House, and American taxpayers.

Any update to FISMA should also require agencies to develop and implement a vendor cyber risk management program that includes third-party contractors and other agencies. Some estimates indicate that more than half of all cyber incidents are perpetrated through a third-party service provider, like the SolarWinds attack was. However, the uniquely interconnected nature of Federal networks means that agencies should also be monitoring their peers' cybersecurity posture. As agencies often share data and work collaboratively across Federal networks, they need to treat a cyber threat to one as a cyber threat to all.

Real-time continuous systems monitoring

The current FISMA requirements include "continuous monitoring" of Federal IT systems. However, agencies currently lack the capability to provide real-time monitoring, relying predominantly on the OMB's quarterly reporting through the Cybersecurity and Infrastructure Security Agency (CISA).

Today's technology environment is dynamic, with agencies leveraging new technologies, like cloud-based applications, AI/ML, quantum computing, and 5G networks. Meanwhile, threat actors continue to deploy attacks against these new technologies. All of this makes relying on static, point-in-time, quarterly reporting insufficient to accurately depict the health of the Federal cyber ecosystem.

Under FISMA 2021, CISA and OMB should incorporate the use of automated technologies that provide dynamic, real-time continuous systems monitoring so agencies can quantify significant cyber incidents that must be reported. Significant cyber incidents must include all major changes to an agency's cybersecurity posture, whether directly or indirectly.

It is now possible to evaluate an organization's cybersecurity risk using data-driven, objective, and continuously evolving metrics. Defining significant cyber incidents with objective metrics based on real-time monitoring provides dynamic visibility into the evolving nature of threats facing Federal networks.

Congress must include a real-time aspect to its FISMA 2021 continuous monitoring capabilities requirements. Without specifying the need for real-time visibility, agencies will continue to be at a disadvantage when trying to protect Federal networks from continuously-adapting, malicious cyber actors.

Conclusion

Learning from last year's data breaches, zero days, cyber espionage campaigns, and ransomware attacks can move Federal agencies toward solutions. With FISMA reform focused on real-time continuous monitoring, agencies can better secure Federal IT systems.

Real-time continuous monitoring enables Congressional oversight committees to provide stronger governance over Federal agencies, and Federal agencies the ability to dynamically assess their relative cybersecurity risk daily. Investments in dynamic visibility solutions for dynamic threats, like security ratings, will better protect our Federal IT systems and save American taxpayers money.

Thank you for the opportunity to provide this testimony.