Cybersecurity Coalition

Testimony of

Ari Schwartz
Venable, LLP
Former Senior Director for Cybersecurity Policy at the National Security Council (2013-2015)

On Behalf of the
Cybersecurity Coalition
and
Center for Cybersecurity Policy and Law

Before the
United States House of Represenatives
Homeland Security Committee
Cybersecurity and Inrfrastructure Protection Subcommittee

"Assessing the State of Federal Cybersecurity Risk Determination"

July 25, 2018

Cybersecurity Coalition

Chairman Ratcliffe, Ranking Member Richmond, and members of the Committee, I am Ari Schwartz. Thank you for the opportunity to appear before you today to discuss our views on the Federal Cybersecurity Risk Determination Report and Action Plan. I do so in my role as Coordinator of the Cybersecurity Coalition, the leading policy coalition of companies that develop cybersecurity products and services.[1]

Over the past decade, the federal government has steadily moved away from "check box compliance" mandates to a risk management approach to address cybersecurity issues. Major steps in this move have included:

- The Cybersecurity Cross Agency Priority (CAP) goals,[2] which ensured that agencies would receive individualized review of their risk management plans;
- The Federal Information Security Modernization Act of 2014,[3] which provided authorities to increase risk assessments of agencies;
- The Cybersecurity National Action Plan, which created a Federal Chief Information Security Officer (CISO) at the Office of Management and Budget (OMB); and
- Perhaps most notably, the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,[4] which required federal agencies to utilize the NIST Cybersecurity Framework[5] to establish a process to manage risk and holds agency heads accountable for doing so.

A risk management approach offers each agency the ability to focus on their specific needs and enables them to demonstrate growth in their cybersecurity efforts while taking steps to address the most critical threats to their mission.

---

[1] About the Center for Cybersecurity Policy and Law and the Cybersecurity Coalition
The Center for Cybersecurity Policy and Law is a nonprofit (501(c)(6)) organization that develops, advances, and promotes best practices and educational opportunities among cybersecurity professionals. The Center provides a forum for thought leadership for the benefit of those in the industry including members of civil society and government entities in the area of cybersecurity and related technology policy. The Center seeks to leverage the experience of leaders in the field to ensure a robust marketplace for cybersecurity technologies that will encourage professionals, companies, and groups of all sizes to take steps to improve their cybersecurity practices. The Center hosts several initiatives focusing on a range of critical cybersecurity issues, including the Cybersecurity Coalition, Better Identity Coalition, and the Hardware Component Vulnerability Disclosure Project.
The Cybersecurity Coalition brings together industry leading companies to share their expertise and unique perspective on critical policy issues, both in the United States and internationally. The Coalition is focused on several active and critical policy issues that require close alignment and coordination to protect the vital interests of the cybersecurity products industry, including: promoting responsible vulnerability research and disclosure; promoting effective privacy processes within cybersecurity policy; establishing government requirements for agency systems; increasing information sharing and threat intelligence; and promoting sound cybersecurity practices in government at all levels. Coalition members include Arbor Networks, AT&T, CA Technologies, Cisco, Citrix, Cybereason, Intel, McAfee, Mozilla, Palo Alto Networks, Rapid7, Red Hat, and Symantec.

[2] *See* Obama Admin. Archives, Cross-Agency Priority Goal Cybersecurity, *available at* https://obamaadministration.archives.performance.gov/content/cybersecurity.html.

[3] PL 113-283

[4] Executive Order 13800

[5] NAT'L INST. OF STANDARDS AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, VERSION 1.0 (2014).

Cybersecurity Coalition

OMB's May 2018 Federal Cybersecurity Risk Determination Report and Action Plan shows that, despite some limited progress, agencies have a lot more to do to effectively manage cybersecurity risk.

This is not an unexpected result. Agencies are not adequately resourced to manage cybersecurity risk, and do not have proper cross-departmental coordination processes to identify and resolve any barriers to achieving this goal. The federal government has not prioritized cybersecurity risk management and simply changing policies to help agencies measure risk will not change their policies on its own.

So what will change agencies' approaches to cybersecurity risk management and drive real improvement? The May 2017 Executive Order had the right idea. It is up to OMB and the President to hold agency leadership accountable to improve.

The OMB Report suggests that Chief Information Officers (CIOs) are not empowered to make the necessary changes and suggests that leadership should empower them to do so. While that is one approach that seems to have worked for some agencies, we would recommend that to really make a change in agencies, senior leadership needs to oversee cybersecurity risk management. In other words, security officers should not be reporting to the CIO, but to the Deputy Secretary or the Secretary. A similar move has started to take place in private companies where CISOs are no longer reporting to CIOs but to CEOs or COOs or directly to the Board of Directors. This shift in thinking has happened because CEOs and Boards of Directors have felt pressure to improve cybersecurity at companies as the result of countless breaches and incidents that have created real and material risk that simply cannot be ignored or delegated to only the information technology teams.

For this to work in the US Government , the Director of OMB, the White House Chief of Staff, and the President must hold the Secretaries directly accountable for cybersecurity risk management at the agencies. Similarly, the Deputy Director for Management at OMB must hold the Deputy Secretaries accountable. Congress must adequately resource agencies and hold the leadership at all levels accountable for managing risk through public oversight. Without this accountability, other measures, however well-intended and necessary, will not be able to succeed to the extent needed to secure our government.

At this point, every agency's leadership has been told that they are responsible for the cybersecurity of their agencies. Agencies have now been measured and have not fared well.

Now is the time to hold the agency leadership responsible for failures and to rapidly address these known cybersecurity risks.