9. Strengthening Federal Cybersecurity

First published as a blog post on February 9, 2017

CAP Goal Statement: *Improve awareness of cybersecurity practices, vulnerabilities, and threats to the operating environment by limiting access to authorized users and implementing technologies and processes that reduce risk from malicious activity.*

During his campaign, President Trump promised to beef up cybersecurity efforts. Press reports on a draft Executive Order from the Administration parallel campaign commitments to launch an immediate review of all US cyber defenses by a Cyber Review Team comprised of individuals from the military, law enforcement and private sector. But his team won't be starting from scratch.

The data breach at the Office of Personnel Management (OPM) in the spring of 2015 was breathtaking in scope—nearly 22 million sensitive personnel records stolen. But this wasn't a new issue. There had been breaches at the FBI, Department of Homeland Security, the IRS, even the National Security Agency.

But the OPM breach was clearly a turning point. It resulted in the removal of the agency head and agency CIO. Yes, federal agencies have been subject to cybersecurity requirements since 2002 under the Federal Information Security Management Act (FISMA). And Congress held periodic hearings excoriating numerous agencies for not complying. Yet, compliance didn't always translate into changes in the day-to-day federal government's culture. This led to the enhancement and expansion of multiple efforts as reflected in the cross-agency priority goal for cybersecurity, which serves as launching point for the new Administration's efforts.

Background. In 2013, the National Institute for Standards and Technology (NIST) convened a public-private sector forum to develop a risk management framework to strengthen cyber defenses. It was published in 2014 as the NIST Cybersecurity Framework and is seen by many in government and industry as the cyber risk management "gold standard." NIST continues to review potential updates to keep the Framework current.

Following the publicity of the OPM breach, the White House launched a 30-day "cyber sprint" in June 2015 to implement high-priority fixes. It also identified critical gaps and emerging priorities that were summed up in a Cybersecurity Strategy & Implementation Plan. Its implementation is being overseen by the President's Management Council, comprised of top agencies' chief operating officers.

A Cybersecurity National Action Plan was released in February 2016. A capstone of seven years of efforts, it assessed cybersecurity trends, threats and intrusions and made a number of recommendations, such as boosting federal investments in cybersecurity to $19 billion (an increase of 35 percent), designating a federal chief information security officer and establishing a Commission on Enhancing National Cybersecurity.

The White House Cyber Commission released its report in December 2016, recommending joint public-private sector action. It developed a set of guiding principles and identified areas for future action, including the importance of the new administration taking action in its first 100 days in order to better equip government to operate in the digital age. It also recom-

mended unifying all federal civilian agencies under a single common network.

A January 2017 report by a bipartisan cyber policy task force sponsored by the Center for Strategic and International Studies spans both public and private sector cyber challenges. It cautioned: "The temptation for grand national initiatives should be avoided, as these usually fall flat." It concluded that any initiatives must be carefully attuned to market forces, have congressional support and not be run out of the White House. It offered recommendations, noting: "We can bring clarity to the task of cybersecurity if we start by assessing what actions create risk." And at that point, specific steps can be proposed to reduce risks by changing behaviors, using incentives—in both the public and private sectors.

The Cross-Agency Goal. Even before the OPM data breach in 2015, the Office of Management and Budget (OMB) convened an interagency team in late 2013 to identify a subset of the FISMA requirements to focus on as one of the 15 Cross-Agency Priority (CAP) Goals. As a result, the goal focused on three sets of risk management initiatives and developed a set of targeted metrics to track progress at a high level:

- *Information Security Continuous Monitoring Mitigation.* The focus is to provide ongoing observation, assessment, analysis and diagnosis of an organization's cybersecurity posture, hygiene and operational readiness.
- *Identity, Credential and Access Management.* The focus is to put in place a set of capabilities that ensure users have legitimate access to IT systems required for their job function.
- *Anti-Phishing & Malware Defense.* The focus is on implementing technologies, processes and training that reduce the risk of malware being introduced through email and malicious or compromised websites.

The metrics are tracked by each agency and centrally reported via the Department of Homeland Security's CyberScope portal, which is used to monitor implementation of FISMA requirements.

Governance Structure. The President's Management Council oversaw the implementation of this goal, and the goal's staff support are located in OMB. In late 2016, the first federal Chief Information Security Officer, Greg Touhill, was appointed and became the point person for the implementation team. However, his scope was broader than just the set of initiatives reflected in the CAP goal. Several subgroups sponsored by the cross-agency Chief Information Officers (CIO) provide support as well. These include a cross-agency Chief Information Security Officers Council and a Joint Cybersecurity Metrics Working Group.

Strategy. The CAP goal was implemented within the context of other, broader cybersecurity initiatives and the dynamics associated with ongoing breaches and incidents. The distinguishing characteristic of the CAP goal, however, is that it focuses more on risk management than on technology fixes. OMB annually issues guidance to agencies describing new initiatives, requirements and priority areas of interest. OMB also convenes periodic "Cyberstat" reviews, which are "deep dive" face-to-face meetings with agency officials to discuss progress within their individual agencies and to develop strategies to better focus resources.

Current Status. While there has been significant churn, there has also been measurable progress, including:

- Designation of a federal chief information security officer to serve as a voice and executive champion for cybersecurity issues within agencies and across the government.
- A governmentwide set of continuous monitoring tools.
- A quarterly scorecard of status and progress by each agency.
- Clarification of the roles and responsibilities of federal agencies in responding to cyber incidents.
- Additional cybersecurity talent hired into government—6,000 in 2016 alone.

Next Steps. The CAP goal has been a useful foundation for several key elements of the broader federal cybersecurity strategy. It provides metrics, insight and oversight of agency efforts. As a result of its efforts, the fiscal year 2017 budget requested a total of $19 billion to support cybersecurity efforts; its approval awaits completion of the pending budget. This includes legislation pending to create an IT modernization fund to replace vulnerable legacy systems.

The federal CIO Council, under the leadership of former federal CIO Tony Scott, offered an assessment of the status of federal IT, including cybersecurity, and recommended future actions, most of which are reflected in existing plans and reports. In addition, Touhill, the former federal Chief Information Security Officer, offered his insight, as well. According to *Federal News Radio,* he concluded: "'agencies don't need any more policies around cybersecurity and technology… In fact, … the Office of Management and Budget had identified 63 policies that needed to be rescinded… ' The success measure is not the number of policies, but how well you execute them."

The new Administration is still putting its agenda in place. According to NextGov: ""An executive order seemingly prepped for President Donald Trump's signature would order four major reviews of the nation's cyber vulnerabilities and capabilities but would not make any immediate changes to U.S. cyber posture."

But a day later, *Federal News Radio* reported that the pending executive order would be more proactive, where: "… department secretaries now will be held more accountable than ever for managing their agency's cyber risks. The draft order would require agency senior leaders to implement the cybersecurity framework developed by the National Institute of Standards and Technology to measure and mitigate risk… Then, the Office of Management and Budget would assess and manage cyber risk governmentwide."

Postscript: President Trump signed Executive Order 13800 in May 2017 to require greater risk management of federal cyber systems, improve the resilience of critical infrastructure in the face of attacks and develop a national workforce with cybersecurity specialties.