Government
Business
Council

Building a
Brave New World

Conversations with Federal Technology Leaders on the Future of Cybersecurity

Underwritten by

vmware®

In the last few months

of 2015, approximately 21.5 million Americans received the following letter: “As you may know, the Office of Personnel Management (OPM) was the target of a malicious cyber intrusion carried out against the U.S. Government, which resulted in the theft of background investigation records. You are receiving this notification because we have determined that your Social Security Number and other personal information was included in the intrusion.”

The 2015 OPM breach marked one of the worst cyber intrusions in U.S. history, and in the years since, the federal government has redoubled its efforts to protect enterprise data — a trend most recently seen in the White House’s 2017 Executive Order promoting cybersecurity reform and modernization.

To explore how organizations are adapting to an increasingly complex threat environment, Government Business Council (GBC) interviewed federal technology leaders on ongoing cybersecurity priorities, pitfalls, and considerations. Together, their observations offer a striking glimpse into one of 21st century government’s most profound challenges: achieving new heights in innovation while safeguarding our nation’s critical IT infrastructure.

What are your organization’s goals regarding cybersecurity?

Sally Holcomb (Deputy Chief Information Officer, National Security Agency): We’ve made a pretty aggressive effort for some years now to improve everything from basic hygiene to enhanced insider threat detection. The overarching goal is, of course, to continue advancing our security measures and stay ahead of what a bad guy could do — but it’s also to understand what technology offers by way of a vulnerability. So in the long term, we’re making it a priority to stay ahead of things and continue evolving. In the short term, we’ve got a number of initiatives under way aimed at improving various fronts: physical security, personnel security, and information and technology security.

> **“The overarching goal is, of course, to continue advancing our security measures and stay ahead of what a bad guy could do — but it’s also to understand what technology offers by way of a vulnerability.**
>
> Sally Holcomb
> Deputy Chief Information Officer, National Security Agency

24th Air Force (24 AF) spokesperson: A crucial effort for cybersecurity in the short term, not just for the USAF but for all components of the Department of Defense, is the push to reach Full Operational Capacity (FOC) for all Cyber Mission Force (CMF) teams. The CMF already is a high-demand, low-density asset engaged in cyber defensive and offensive missions on behalf of USCYBERCOM. The Air Force’s contribution of 39 teams is scheduled to reach 100% FOC status in September 2018.

In the long term, 24th Air Force has begun implementation of three key transformational efforts which will transition us from a network-centric force to a cyberspace force centered on operations and mission assurance for the commander. These three major efforts include evolving toward the Air Force Information Dominance Platform (AFIDP), maturing and resourcing our SAF/CIO-piloted Cyber Squadron Initiative and Inherent Mission Defense Teams (MDTs), and, finally, the development and fielding of the Air Force Materiel Command's Cyber Resiliency of Weapons Systems (CROWS) Office capabilities. These three major endeavors deliver a coherent approach to cybersecurity, cyber defense, weapon system resiliency, and the critical "every Airman a sentry" cyber hygiene culture across our Air Force.

Melinda Rogers (Chief Information Security Officer, Department of Justice): At the Department of Justice, we are focused on minimizing vulnerabilities, providing real-time detection and response, implementing rapid analysis and forensics, and protecting our high-value assets. We've made significant investments in tools and technologies, enhanced internal policies and processes, and top talent.

What are the chief challenges and considerations you're navigating with regard to modernizing cybersecurity?

Sally Holcomb (NSA): Broadly speaking, the external and internal threat vectors haven't changed all that much — dealing with an adjusting landscape of what individual technologies provide and create is the part that actually shifts. The vulnerabilities themselves change, but the actual threats haven't changed. As the technology landscape evolves, so do the ways an adversary has of messing with you. You have to understand what you're doing while you modernize to ensure that you're addressing the new avenues, the new vectors, that the threat can take. Every time you modernize, you also create new avenues — that's always been a challenge, and we're continuing to work through it. For us, the big challenge is achieving a proper balance between mission agility and security: ensuring that we have the means to prevent those threats from coming to us, but at the same time ensuring that our workforce is able to execute operations in a free flow fashion. And those two sometimes are directly opposed.

> **"Broadly speaking, the external and internal threat vectors haven't changed all that much — dealing with an adjusting landscape of what individual technologies provide and create is the part that actually shifts.**
>
> Sally Holcomb
> Deputy Chief Information Officer, National Security Agency

Part of dealing with this reality is simply communicating the need to adjust over time. As problems arise, we have to make it clear that the pendulum may swing — it may be that security gets more prioritization at certain times than it does at others. It helps if you have unlimited time and money, but that never seems to be the case in government. So we are just constantly, with every initiative we pursue, looking at that trade-off between hampering agility and the improving security. Every single initiative involves that calculus.

24 AF spokesperson: Working within the federal acquisition cycle is a major consideration with regard to remaining at the peak of cyber readiness. The cyber terrain changes on an almost daily basis; however, the traditional process by which government entities adopt new technologies can take months or years. Initiatives such as the Cyber Proving Ground have already been established to rapidly acquire innovative technologies from industry, but if the Air Force wants to remain a dominant player within the cyber domain, the process by which we field new technologies needs to be readdressed with adaptability and efficiency in mind.

Melinda Rogers (DoJ): The threat landscape is constantly evolving, and attacks are becoming increasingly sophisticated and more frequent. In response, we are constantly evaluating new technologies to automate and optimize our response. As part of our risk management framework, we prioritize and reassess our cyber investments.

> “The cyber terrain changes on an almost daily basis; however, the traditional process by which government entities adopt new technologies can take months or years.
>
> — 24th Air Force spokesperson

What is your organization’s strategy with regard to containing and minimizing the impact of cyber breaches?

Sally Holcomb (NSA): The challenge is, how do you ensure the appropriate protections to track what a privileged user is doing while also enabling them to work without the overhead of constantly having their activities watched? It’s that agility versus security problem — we need to strike a balance in that area.

With regard to data recovery and damage control, we take the same approach that anyone would: containing the initial crisis, then figuring out the vulnerability that permitted the crisis, and, finally, looking at future improvements you can make based on what you’ve learned.

24 AF spokesperson: The Department of Defense presented its cyber strategy in 2015, which laid out three primary

VMware Perspective

According to Matt Schneider, Senior Director of the U.S. Public Sector at VMware, the federal government has reached a critical juncture in data security.

"When it comes to cyber defense, government has traditionally prioritized infrastructure protection — but that's no longer enough," he observes. In the face of expanding volumes of critical data, organizations must be capable of quickly detecting and containing threats. That's easier said than done, however: the sheer amount of data that security teams are forced to wade through means that they're often unable to respond appropriately to alerts.

To illustrate this, Schneider compares the data center to a gated community: "Right now, the alerts customers receive essentially amount to a call notifying the security guard of bad behavior somewhere in the neighborhood. They're not provided with any specifics, meaning the guard is just wandering around without any idea of what the bad behavior is or where it's taking place."

This contributes to an unacceptable lag in response time. Instead of going in blind, organizations must be able to hone in on a threat's nature and location — and this means shifting defenses to the application itself. By implementing core cybersecurity principles of least privilege, micro-segmentation, multi-factor authentication, encryption, and patching at the application rather than infrastructure level, organizations can limit exposure and increase the likelihood of protecting subsequent locations. Ultimately, these elements will empower government to take a more risk-based approach and actively protect critical applications, ensuring "known good" rather than constantly searching for bad actors. After all, says Schneider, "breaches are going to occur — but by developing a comprehensive understanding of application performance, of who should be accessing applications, of how to protect applications at a deeper level, we can maintain and improve upon security levels."

Matt Schneider

Senior Director of the U.S. Public Sector, VMware

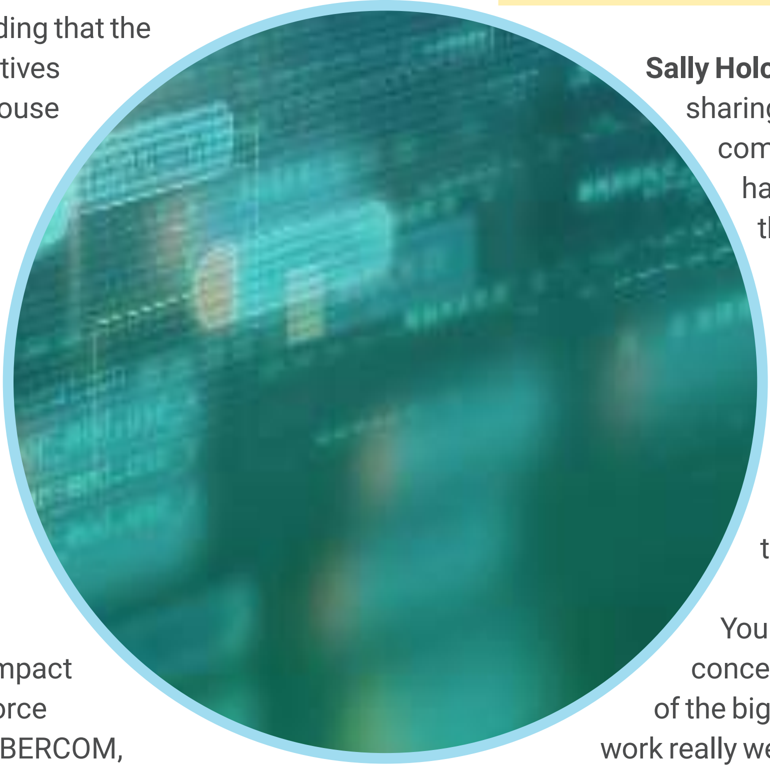
missions: to Defend our networks and ensure data is held secure; to support joint military commander objectives; and, when directed, to defend U.S. interests in cyberspace.

Our first line of defense against cyber breaches is to create an impenetrable network. Our Weapons Systems secure the AFNet against more than 1.3 billion attempted malicious connections annually, while our Cyber Airmen patrol the network to defend it against any threats that may have slipped through the cracks. This multilayered approach to cybersecurity allows for rapid recognition, isolation, and neutralization of threats. Moving forward, initiatives such as the SAF/CIO Cyber Squadron Initiative, which places cyber operators inside Wing organizations, and the Mission Defense Teams will increase our awareness of the network's baseline so that abnormal activity can be detected with ever more speed and precision.

Melinda Rogers (DoJ): One key component of our strategy is to be proactive and prevent the breach from occurring at all; we're also continuously reducing the time it takes to respond and remediate a cyber breach. We're accomplishing this by automating incident response management and by standardizing IT across the organization to reduce the complexity and the vulnerability footprint. This standardized IT environment will allow for better information sharing, expedited incident response, and simplified operations and maintenance.

What impact do you expect from the White House's increased prioritization of modernization and cybersecurity?

Sally Holcomb (NSA): Between the IC IT Enterprise (IC ITE) and all of the other security initiatives we've been working on for years, we're finding that the executive orders and the directives we're seeing from the White House tend to actually support what we've been working on and provide the foundational doctrine that we're already acting upon. So I don't really expect to see an impact, per se — it just helps provide backup support from a policy perspective.



24 AF spokesperson: The cyber sphere is continuing to mature, and an increased appreciation for its potential impact is to be expected. As the Air Force component provider for USCYBERCOM, 24th Air Force will continue to modernize and build in order to provide mission assurance for the combatant commander. We're focused not only on posturing ourselves for today's fight, but remaining dominant in tomorrow's fight.

Melinda Rogers (DoJ): Cybersecurity and IT modernization are key DoJ initiatives — having this message come from the Executive Office reiterates the importance of safeguarding our IT assets across the federal government landscape.

Can you tell us about any recent cybersecurity modernization initiatives that have succeeded or failed?

Sally Holcomb (NSA): We spend a lot of time sharing lessons learned with others in the community and across the DoD — we've had some missteps, some things that we thought might be good, but you don't actually know until you implement it. So we'll go out and let people know, "Hey, this product or activity turned out not to have the bang for the buck that we'd initially thought." We've focused on ensuring that others are aware in order to save them trouble — we all need to do that.

You can have problems arise in both the conceptual and implementation phases. One of the big challenges is that vendor products work really well in standardized, homogenous environments — but you seldom find one of those in the intelligence community. So you often go down a path where you launch a particular product and only find out later that you can't get it effectively to implemented across the environment.

24 AF spokesperson: A recent major success story would be the introduction of the Automated Remediation and Asset Discovery (ARAD) platform to our unclassified network. This technology utilizes a linear, peer-to-peer query system that allows operators to see in seconds what previously would have taken days or weeks — it's already proven vital in managing and remediating endpoint vulnerabilities. ARAD was adopted as a military utility assessment (MUA) of the commercial Tanium product, and it represents a success story where collaboration between AFLCMC, AFSPC, 24AF, and Air National Guard enabled us to rapidly acquire and implement a new platform across all portions of the Air Force-controlled DoD unclassified network.

Melinda Rogers (DoJ): I'm proud of the strong DoJ-wide support for cybersecurity and the commitment from our mission components. We're going to continue investing in our cyber capabilities to ensure that our assets are properly safeguarded. Our goal is continuous improvement and innovative solutions for our cyber protections and incident response capabilities, and we'll stay the course.

Research Methodology

GBC and VMware launched a qualitative research campaign in July 2017. From August 1, 2017 to September 6, 2017, GBC conducted interviews with federal government technology leaders on topics surrounding organizations' cybersecurity modernization initiatives. The list of featured interviewees is as follows:

Sally Holcomb — Deputy Chief Information Officer, National Security Agency (NSA)

Melinda Rogers — Chief Information Security Officer, Department of Justice (DoJ)

Spokesperson — 24th Air Force (24 AF)

Government Business Council

About Government Business Council

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 40 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

vmware®

About VMware

VMware, a global leader in cloud infrastructure and digital workspace technology, accelerates digital transformation by enabling unprecedented freedom and flexibility in how our customers build and evolve IT environments. With VMware solutions, organizations are improving business agility by modernizing data centers and integrating public clouds, driving innovation with modern apps, creating exceptional experiences by empowering the digital workspace, and safeguarding customer trust by transforming security. VMware is a member of the Dell Technologies family of businesses.