

Strengthening Federal Cybersecurity Capabilities

**How the Department of Education, NASA, and FEMA are
safeguarding some of the nation's most sensitive assets**

Underwritten by



Cybersecurity is one of the most formidable information technology (IT) challenges of the present day, and its repercussions in the public sector cannot be overstated. While a security breach in a commercial organization can lead to leaked financial information, a similar breach in a government entity can result in disclosure of personally identifiable information (PII) that jeopardizes citizen safety and trust in government institutions. Most recently, Customs and Border Protection (CBP) was hacked in a successful malicious effort that obtained photo, video, and other identifiable data — the data were eventually made public online.¹

Although there is consensus about the importance of cybersecurity, questions remain as to the precise execution of cybersecurity goals — how, exactly, can government achieve the digital protection required to thwart the attacks of today's threat landscape? And what are the most effective ways of achieving such an outcome? To answer these and other critical cybersecurity questions, Government Business Council (GBC) conducted a series of interviews with leading experts across a number of agencies.

Read more to learn what federal government experts at the Department of Education, NASA, and FEMA are doing to safeguard the nation's most sensitive cyber assets.

“Right around 90% of the successful attacks we see, especially from a threat intelligence perspective, are coming in through phishing.”

— Steven Hernandez
Chief Information Security Officer, Department of Education (DOE)

Department of Education: Cybersecurity as the Foundation for Mission Success

What are the cybersecurity implications of consolidating millions of student records, billions of dollars in student loan disbursements, and thousands of linked educational institutions? To understand the scale of the Department of Education's mission, GBC spoke with chief information security officer (CISO) Steven Hernandez about his organization's mission to protect student information. “When we look at Federal Student Aid, we have a \$1.5 trillion portfolio in terms of accounts receivable. We issue hundreds of billions of dollars in educational funding and grants every single year and maintain the risk of that portfolio.”


The intersection of those data points creates nodes of vulnerability, but it does not necessarily create a transparent ‘data lake’ that can be observed and inspected by a centralized team at the Department — a challenge that Hernandez and his staff are grappling with. These varied data sources often live in disparate and disjointed sites throughout the Department of Education's digital universe, so extrapolating unified and timely insights is often an uphill battle.

Hernandez also speaks to the changing dynamics that underpin the security of an entire federal department's cyber assets. Because security tools have developed over time, nefarious actors often strike at what Hernandez describes as “the loosest link in the chain” — the IT network's ‘end users,’ or employees.



Attackers are assuming that at least one or more employees will click an email link that appears to originate from a trusted source, unwittingly granting access to those without authorized privileges.

This dynamic is not unique to the Department of Education. Just last year, the Federal Bureau of Investigation and the Office of the Director of National Intelligence released the Insider Threat Program Maturity Framework to help agencies coach personnel on identifying suspicious user activity and common tactics that exploit user credentials.² And with the prospect of 5G network technology on the horizon, government networks are likely to experience even more pressure going forward.³ Fortunately, Hernandez posits, there are frameworks to enable individual end users to identify and prevent threats before critical damage takes place:



“Through progressively difficult phishing exercises, we’ve seen demonstrable improvement to the point where, during our last phishing exercise in which we targeted about 6,000 accounts, we had five people actually click the link and take the bait. Two years ago, that would have been as high as about 20% of our organization. When we start to blend the idea of front-end technologies, training and security awareness, ‘live fire’ testing and training with our phishing exercises, and that executive support messaging, we see

a drive towards positive change.” Given existing cybersecurity trends and the immensely disastrous ramifications of data breach at the Department, this achievement speaks to the tangible ways in which government can build a savvier workforce in control of its own digital destiny. Despite notable victories, CISO Hernandez maintains a number of concerns when it comes to implementing cybersecurity practices, even sharing specific recommendations for the Department’s commercial cybersecurity partners:

“When you look at our portfolio as a whole, it’s a tremendous amount of financial information systems that contain data about students, including PII. Where we work with disabled veterans to get them educational opportunities, we have some of their medical history.”

— Steven Hernandez
Chief Information Security Officer, Department of Education (DOE)

“A real challenge that we see right now is we have a lot of tools and capabilities. We’ll collect the data, but you’re not going to get the data out in a native API type of interface. You’re not going to be able to tie the data you’re collecting through our platform into a big data capability where advanced analytic tools become available. Those are becoming very challenging conversations because having a myopic view is not going to be sufficient for me to manage risk in my organization.”

NASA: Managing Risk at an Agency Built for Exploration

The National Aeronautics and Space Administration (NASA) is no stranger to risk and exploration. The agency that spearheaded America's mission to the moon was also the first to measure cosmic rays in Earth's atmosphere, and who most recently landed, operated, and maintained communication with a space vessel that explored the furthest reaches of the solar system. Even in this context, cybersecurity leaders like NASA chief information officer (CIO) Mike Witt acknowledge that some risks are not worth taking. According to Witt, the role of the office of the CIO is to "understand what our risks are, what the missions are trying to do and how we can help things succeed and take risks, but also to protect the rest of our enterprise and the rest of our missions if one of the missions is going to take on a significant amount of cyber risk."

Witt's experience working with the Department of Homeland Security and Internal Revenue Service prior to joining NASA fed directly into process innovations aimed at diminishing the siloed mission culture that defined NASA and can be found at other federal agencies. This has included standing up a program by which security professionals gain direct experience at peer agencies as well as being able to exchange trade insights, analytical tools, and develop contacts for navigating future security challenges. "We have our personnel that work in security operations work at another agency for a week or two, and then vice versa, we bring that security analyst to our

environment. It gives the other agency a perspective that they do not have otherwise, and you start building trust amongst the operational employees."

The approach on display at NASA may be just what other federal agencies need to adopt in order to prevent attacks like the one perpetrated on the Office of Personnel Management in 2016.⁵ It will take a national effort to thwart today's malicious insiders and prevent tomorrow's adversarial nation threats.

"[The CIO's role is to] help things succeed and take risks, but also to protect the rest of our enterprise."

— Mike Witt
Chief Information Office, National Aeronautics and Space Administration (NASA)



FEMA: Using Cybersecurity to Defend Against the Uncontrollable

Kenneth Kline, IT Manager at the Federal Emergency Management Agency (FEMA), paints a picture of a government organization accustomed to fighting the nation's most destructive cybersecurity offenders.

On a typical day, FEMA's cybersecurity environment largely resembles that of the Department of Education, NASA, and other comparably sized federal agencies. But on days when emergencies strike — a hurricane making landfall, tornadoes touching down, or severe flooding — FEMA's IT mission changes dramatically. Suddenly, the agency's digital infrastructure can balloon to several orders of magnitude larger than its typical scale, encompassing state and local emergency response professionals, first responders, healthcare professionals, and other stakeholders who require reliable channels for information.⁶ According to Kline, cybersecurity is the tether that binds these individual IT components together and prevents the injection of a digital disaster alongside a natural disaster.

On top of this, FEMA must preserve "visibility of traffic flows" for "detecting malware on individual

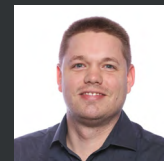
Expert Perspective from Google Cloud

With PII and other sensitive data spread across government and commercial entities, today's cyber challenges point to the need for an ecosystem that provides security in depth, from data center to device. This ecosystem must provide intuitive, yet rigorous technical controls that ensure a manageable, accessible workload for each end user.

The training efforts undertaken at the Department of Education as well as the protocols implemented at NASA and FEMA are steps in the direction of a necessary transformation. Effective IT modernization hinges on integrating sophisticated security capabilities directly into the enterprise. Given the evolving threat landscape, these security capabilities must provide defense-in-depth, protecting an organization's data, applications and users at scale.

Platforms like Google Cloud are continually evolving to protect against an ever-changing threat landscape while also providing customers best-in-class security and machine learning tools to meet this need.

While industry is developing and implementing many of the technologies that underpin existing cybersecurity efforts, it will be critical for specific agencies and government-wide bodies to collaborate with technology providers in framing out the path to readiness. In tandem with technology partners, public sector agencies can elevate the federal government's security posture to meet the evolving threats of today's (and tomorrow's) malicious actors as well as the functionality needs of the modern workforce.



Scott Fleming

*Head of Google Cloud Professional Services,
Public Sector and Security*



devices and cutting that device off from the rest of the network to prevent spreading.” Kline further mentions the centrality of cloud tools in meeting what he calls “a large volume of activity” that can potentially arise during a disaster: “That’s where some of the wins from the cloud are — we now have the ability to spend and pay for what we need and scale applications, or develop systems and tap some of the security features from the ground rather than trying to bolt it on at the end.”

According to Kline, staying abreast of innovative tools like cloud technology and newly developed security protocols allows FEMA to maintain a rigorous security posture while preparing for incredibly strenuous emergency situations. The incorporation of these tools allows the agency to meet broader federal initiatives for technology modernization within its cost constraints and security demands.

Conclusion

The federal government faces constantly evolving security threats from all sides, complicated by greater sophistication of cyberattacks and intrusion methods. Cybersecurity leaders are working vigilantly to implement the technical and personnel strategies that can remove existing vulnerabilities, but success on this front will likely require enhancing ongoing efforts while improving collaboration across agencies and mission assignments.

Research Methodology

Government Business Council (GBC) and Google Cloud launched a qualitative research campaign in March 2019. From April to May 2019, GBC conducted a series of interviews with federal leaders in information technology and cybersecurity. The list of featured interviewees is below.

Steven Hernandez — Chief Information Security Officer at the U.S. Department of Education

Kenneth Kline — Information Technology Manager at the Federal Emergency Management Agency

Michael Witt — Chief Information Officer at the National Aeronautics and Space Administration



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.

Report Author: Igor Geyn

Endnotes

1. Washington Post: "U.S. Customs and Border Protection says photos of travelers were taken in a data breach." June 10, 2019. https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/?utm_term=.25107f2557ed
2. Cyberscoop: "Federal insider-threat programs get a dose of 'Maturity'." November 1, 2018. <https://www.cyberscoop.com/insider-threat-task-force-maturity-framework/>
3. Business Insider: "AI and 5G will create an explosion in cybersecurity risks, says FBI agent and general counsel at \$50 billion firm." May 18, 2019. <https://www.businessinsider.com/ari-mahairas-and-peter-beshar-on-ai-and-5g-security-risks-2019-5>
4. National Aeronautics and Space Administration (NASA): "NASA History Overview." April 2, 2018. <https://www.nasa.gov/content/nasa-history-overview>
5. CSO Online: "The OPM hack explained: Bad security practices meet China's Captain America." November 6, 2018. <https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html>
6. Government Business Council: "When Someday is Today: Lessons for Health Security and Disaster Mitigation." December 2017. [http://cdn.govexec.com/media/gbc/docs/when-someday-today-lessons-health-security-and-disaster-mitigation_\(1\).pdf](http://cdn.govexec.com/media/gbc/docs/when-someday-today-lessons-health-security-and-disaster-mitigation_(1).pdf)



About Google Cloud

Google Cloud is widely recognized as a global leader in delivering a secure, open, intelligent, and transformative enterprise cloud platform. Our technology is built on Google's private network and is the product of nearly 20 years of innovation in security, network architecture, collaboration, artificial intelligence, and open source software. We offer a simply engineered set of tools and unparalleled technology across Google Cloud Platform and G Suite that help bring people, insights, and ideas together. Customers across more than 150 countries trust Google Cloud to modernize their computing environment for today's digital world.