Modern Authentication for the Federal Government

Enabling Mobile, Secure Authentication in Zero Trust Environments

Jeremy A. Grant
Managing Director of Technology Business Strategy

Grant Schneider
Senior Director of Cybersecurity Services

Jamie M. Danker
Senior Director of Cybersecurity Services

Ross B. Nodurft
Senior Director of Cybersecurity Services

July 29, 2021
For Yubico

VENABLE LLP

Executive Summary

The COVID-19 pandemic has changed the federal IT landscape in the past year, causing a dramatic shift to remote work and an increased use of mobile and personal devices. In these new operational environments, the network edge dissolves, and digital identity, authentication, and access management matter more than ever. Federal agencies' pivot to cloud services to enable remote collaboration, coupled with the use of unmanaged mobile devices, has provided hackers with significant new opportunities to exploit credentials. Furthermore, as seen in the SolarWinds attack, identity and authentication remain a major attack vector, prompting the Biden administration to issue Executive Order (EO) 14028, Improving the Nation's Cybersecurity. The EO mandates agency adoption of multi-factor authentication and implementation of Zero Trust architecture. To address EO mandates, agencies can leverage funding appropriated by Congress from the Technology Modernization Fund (TMF) and for shared services provisioned by the Cybersecurity and Infrastructure Security Agency (CISA) while prioritizing cybersecurity in their annual budget requests.

While the Personal Identity Verification (PIV) and Common Access Card (CAC) smart card standards remain prevalent throughout the federal government, the need to move beyond PIV and CAC for authentication has never been greater. In the Zero Trust environments that agencies are building, the diversity and number of endpoints accessing pieces and parts of an agency network will likely increase. The proliferation of mobile devices is not well suited for PIV/CAC cards, and long-standing issuance challenges remain. Following the 2015 Office of Personnel Management data breach and a renewed push for mandatory PIV use, 15-20 percent of agency populations that could not take advantage of PIV cards to secure their systems have, in many cases, been relying on nothing more than usernames and passwords. Yubico, a global authentication leader, is uniquely positioned to provide flexible security to address these agency challenges with their core invention — the YubiKey, a small USB and NFC hardware security key that secures access to IT systems and online services.

- Mobile Device Authentication: *Derived PIV and FIDO* – As a FIPS 140-2 validated hardware token capable of emulating PIV/Smartcard functionality and enabling authentication via one-time password and modern authentication protocols such as FIDO U2F and FIDO2 via a single security key, YubiKeys can help users authenticate for entry into multiple environments across multiple devices that span a broad spectrum of risk, and help fill some of the gaps caused by the federal government's "PIV or nothing" approach to authentication
- Authentication for the "PIV-less"– YubiKeys are flexible and can be issued broadly, including to contractors, detailees, and seasonal employees – populations the federal government has historically struggled to issue PIV cards to. By using modern FIDO authentication standards and remote/virtual proofing services, YubiKeys can provide the equivalent authentication assurance level 3 and identity assurance level 2. YubiKeys can store up to 25 credentials on a single hardware token, allowing for security authentication across multiple accounts. In addition, YubiKeys can work with almost any type of device or operating system through USB and NFC, enabling secure authentication regardless of the type of working environment. This also means YubiKeys can help fill the authentication gap in instances where individuals have a PIV/CAC card but can't use it to access a particular system or application

As agencies implement EO requirements to implement MFA and zero trust, they should include deployment of YubiKeys as part of their strategy.

Current Landscape

The COVID-19 pandemic broke down barriers and forced dramatic shifts in the ways in which we do business and interact with one another. Digitalization of services, shifts in workforce culture, and the increased use of mobile and personal devices[1] have all helped the federal workforce adapt to a daily routine that enables safe social distancing.

As the United States begins to turn the corner on the pandemic, it is clear that telework is here to stay – not just in the private sector, but in federal agencies as well. The Biden administration has indicated that most agencies are likely to embrace hybrid models where many workers split their time between home and office.[2]

In line with a more mobile, virtual workforce, the overall use of collaboration tools has increased significantly. According to a McAfee report,[3] enterprise use of collaboration cloud services more than doubled from January 2020 through April 2020. During the same period, McAfee saw the use of unmanaged devices more than double. This pivot to cloud services to enable remote collaboration, coupled with the use of unmanaged mobile devices, has provided hackers with significant new opportunities, particularly through the exploitation of new cloud credentials.[4] The report indicates that threat events in public sector cloud accounts during that same time period increased by 773 percent. These events include "excessive usage from anomalous locations" and "login attempts from more than one geographically distant location."

Public Sector Workforce Trends*

100% Increase
Enterprise use of collaboration cloud services

100% Increase
Use of unmanaged devices

773% Increase
Threat events in public sector cloud accounts

*January – April 2020

While these statistics demonstrate an increase in threat events during the height of the COVID-19 pandemic, many agencies have indicated that these trends will continue. The Office of Personnel Management (OPM) has granted flexibility[5] to federal managers on their use of telework, and many managers have seen an overall increase in both productivity and job satisfaction. This means that, across the country, both federal and private sector workforces have pivoted to mobile, cloud-based environments, and this model is here to stay. This provides significant opportunities for hackers – through identity-focused attacks – to gain access to these newly architected environments.

Software Supply Chain Attack and Government Response

Supporting remote work has always presented challenges, but adversaries upped the ante this past year, as demonstrated by the SolarWinds attack. In the spring of 2020, the Russian intelligence service launched a cyberattack by embedding malicious code in a software update of a widely used information technology management platform. Once the hackers gained administrative privileges in a network, they took control of the token signing certificate to generate authentication tokens and gain access to emails and other information across federal departments and agencies. According to the Deputy National Security Advisor for Cyber and Emerging Technology, Anne Neuberger, nine federal agencies and about 100 private sector entities were impacted by the incident.[6] Given the focus of the attack, a CISA executive in March proclaimed "Identity is everything now. . . .

[1] https://www.prnewswire.com/news-releases/us-study-finds-covid-19-pandemic-transforms-cell-phone-usage-301066502.html

[2] https://www.whitehouse.gov/wp-content/uploads/2021/06/M-21-25.pdf

[3] https://www.mcafee.com/blogs/enterprise/cloud-security/working-from-home-in-2020-how-cloud-use-changed/

[4] https://www.csoonline.com/article/3545775/use-of-cloud-collaboration-tools-surges-and-so-do-the-attacks-report-shows.html#:~:text=The%20use%20rate%20of%20certain,education%20ranked%20at%20the%20top

[5] https://www.whitehouse.gov/wp-content/uploads/2021/06/M-21-25.pdf

[6] https://www.meritalk.com/articles/solarwinds-hack-compromised-9-fed-agencies-executive-action-on-the-way/

> “ …identity has become the boundary, and we need to start readdressing our infrastructures in that manner.[7]

The SolarWinds attack on the digital identity layer of government infrastructure led to the development and release of Executive Order 14028, Improving the Nation’s Cybersecurity.[8] The EO focuses agency efforts on shoring up cybersecurity business processes – including identity and authentication – and requires additional investments by departments and agencies in cybersecurity tools and services. Specifically, in response to the requirements of the EO, NIST has published the requirement that all users and administrators of software and software platforms deemed “critical” under the NIST definition must use multi-factor authentication that is resistant to verifier impersonation. SolarWinds and the follow-on EO have significantly impacted both Congress’s and the Biden administration’s approaches to cybersecurity.

Congressional and Administration Approach to Identity-Related Impacts of Solar Winds and EO 14028

Impact Area	Description
IT Modernization	The administration and members of Congress recognize that the country can no longer put off the modernization of the government’s legacy information technology infrastructure. This legacy architecture, coupled with the decentralized management systems that govern its security, has left too many security gaps across the federal enterprise
Zero Trust Architecture	As agencies modernize their infrastructures, they must architect their new environments using Zero Trust security models (as defined in the EO)
Multi-Factor Authentication	Use of multi-factor authentication (MFA) is an essential component of any Zero Trust security model, and the EO mandates that agencies implement MFA everywhere within 180 days (by November, 2021)
Funding Sources	Agencies – through congressional funding – must provide the resources to make sustained investments to achieve these more modern, Zero Trust environments. While some money is available through emergency funding and current budgets, this process will take several years to resource appropriately

While the impacts of the SolarWinds attack are still being researched, the scope and scale of the incident have galvanized the government to respond by increasing the level of security across the federal enterprise. Between the rapid shift to cloud technology enabling telework and the move to modernize using Zero Trust security principles, the government is poised to make significant structural and long-lasting changes to federal environments that will rely on secure digital identity infrastructure, governance, and authentication.

As identity and security operators at federal departments and agencies consider the best way to mitigate these attacks and implement those changes, they must make investments in technology while modernizing traditional IT business processes. Later in the paper, we present a use case around a risk-based approach to mobile authentication. Appendix A provides an overview of federal identity, credential, and access management (ICAM) policy and guidance.

Federal Identity Funding

Resource constraints continue to slow agency modernization efforts, including those related to authentication. However, in the wake of COVID-19 and SolarWinds, the Biden administration and Congress have worked together to provide emergency funding focused on modernization and cybersecurity. Additionally, agencies have had a year to build funding requirements into fiscal year (FY) 2022 budget requests and will look to develop them further in upcoming budget cycles. Below are several areas of potential funding agencies can leverage to meet the cybersecurity, modernization, and identity requirements in the executive order.

[7] https://federalnewsnetwork.com/cybersecurity/2021/03/cisa-identity-is-everything-for-cyber-defense-post-solarwinds/

[8] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

Potential Federal Funding Sources for Federal Identity

Source	Agency-Defined	Description
Technology Modernization Fund (TMF)	$1 billion	In response to the American Rescue Plan (ARP), Congress appropriated $1 billion in TMF money. OMB then issued new TMF guidance in May 2021, prioritizing the use of TMF funds for projects that move "towards a 'zero trust' architecture"
American Rescue Plan (ARP) Funding	$650 million	In addition to the TMF funding, Congress appropriated $650 million for CISA to meet several EO requirements through the Continuous Diagnostics and Mitigation (CDM) program
Agency-specific budgets	$750 million	Agencies have asked for some additional cybersecurity, digital identity, and modernization money in FY22. Additionally, DHS has requested an increase above FY21 levels to include a $750 million fund to meet EO requirements
Future budgets		Beyond FY22, agencies will look to budget for modernization, identity, and security to meet the requirements that they will define in their Zero Trust roadmaps. Expect to see the implementation of this executive order over the next two to three budget cycles (FY23-FY24)

These buckets of funding will be critical areas of opportunity for agencies interested in pursuing upgrades to their ICAM infrastructure as they transition to more modern, cloud-based environments.

Yubico and a Modern Approach to Authentication

We can see from the drivers listed above that the federal government is being both pushed and pulled into a cloud-based virtual working environment faster than ever before. The federal IT environment post-COVID-19 will not look like it did pre-pandemic. Modernization and adoption of Zero Trust architectures will ramp up, while federal telework policies and virtual work environments are likely to expand.

That normalization of virtual work environments will open the door for the use of a greater number and wider array of mobile devices. This move beyond the traditional enterprise boundary will allow employees to engage in transactions that span the gamut of risk; and they will engage in those transactions from a greater number of mobile devices and locations.

> In these new operational environments, the network edge dissolves, and digital identity, authentication, and access management matter more than ever. In the Zero Trust environments that agencies are building, the diversity and number of endpoints accessing pieces and parts of an agency network will likely increase. However, agencies can embrace this change by elevating the importance of more modern, risk-based approaches to multi-factor authentication and leveraging new form factors and authentication protocols beyond the PIV and CAC card.

We expect solutions like the YubiKey to play a significant role in this next phase of federal authentication infrastructure. As a FIPS 140-2 validated and DOD OCIO approved hardware security key capable of not only emulating PIV functionality but also enabling authentication via FIDO2, FIDO U2F, and one-time password (OTP) protocols, YubiKeys are ideally positioned to help fill some of the gaps caused by the "PIV or nothing" approach to authentication.

YubiKeys Mitigate Agency Risk

YubiKeys have been a staple in the federal environment for years. In 2017, the Department of Defense (DoD) issued a policy memo approving YubiKeys as an alternative MFA solution for applications where DoD PKI authentication was not supported.[9] Today YubiKeys are even more well positioned to help mitigate some of our nation's most pressing threats. Currently, nation-state actors and sophisticated, state-sponsored criminal organizations are targeting the supply chains of both hardware and software products and services. YubiKeys are manufactured in the United States and are FIPS 140-2 validated, making them well positioned to mitigate risks that come along with embracing a more mobile, virtual workforce.

[9] See https://www.serdp-estcp.org/content/download/48069/457866/file/20170414_RSA%20and%20YubiKey%20Memo_Signed.pdf

Additionally, YubiKeys can meet all authentication assurance levels (AALs), as enumerated in NIST SP 800-63-3. Agencies have been using them in some cases to bridge the gap between PIV/CAC cards and mobile devices, since YubiKeys can interface with mobile devices over both USB and NFC interfaces. With support for PIV, FIDO2, FIDO U2F, and OTP authentication modes, a single YubiKey can be used to authenticate for entry into multiple environments and across multiple devices that span a broad spectrum of risk.

Below are two use cases that agencies may consider when considering what type of multi-factor authentication form factor to deploy across the enterprise.

Use Case #1

Mobile Device Authentication – Derived PIV and FIDO

Since 2004, the federal government has mandated the use of "secure and reliable forms of identification."[10] This mandate, Homeland Security Presidential Directive 12 (HSPD-12), defined strong authentication as being "based on sound criteria" for identifying an employee and "strongly resistant to identity fraud" and other forms of tampering, allowing for rapid electronic authentication, and being "issued only by providers whose reliability has been established by an official accreditation process." Over the last 18 years, the federal government has relied on PIV cards underpinned by OPM-approved credentialing authorities. However, our computing environments have changed significantly over the last two decades. They have even changed significantly in the last six years since the OPM breach, which led to a government-wide push to fully issue and utilize PIV cards.

This means the proliferation of smaller, mobile, highly capable "mobile" computing devices that combine computing workstations, telephones, and electronic organizers. Accelerated by the pandemic, federal employees have turned to laptops, tablets, and smartphones to communicate and collaborate without face-to-face interaction.[11] Security researchers have seen an over 50 percent increase in the use of "unmanaged devices" across industry verticals to include government. While PIV cards can be leveraged in laptops (through use of sleds), they become harder to use as personal devices become smaller. NIST recognized this impracticality through its guidance on issuing of derived PIV credentials.[12] In doing so, however, they recognized software-based derived PIV credentials at a lower level of authentication assurance than a hardware-based authenticator.

This is where use of YubiKeys becomes extremely helpful for agency ICAM leaders, CIOs, and CISOs. Yubico has partnered with Entrust to provide derived PIV/CAC credentials on YubiKeys, aligned with NIST standards.[13] This means that a single, portable, hardware-based authenticator can provide the same level of authentication assurance (AAL3) across multiple mobile devices, applications, and web browsers. Given the reporting of phishing of mobile authenticators,[14] use of a hardware-based cryptographic secret can protect employees from the risks associated with phishing, man-in-the-middle, sim-swapping, and other mobile authenticator attacks. There are several other important points to note about the use of YubiKeys to securely authenticate across mobile devices.

Benefits to Using YubiKeys with Mobile Devices

- Works with all of the leading operating systems and mobile device platforms
- Ability to be plugged into devices or use near-field communication
- Agencies have the flexibility to layer on several different attributes – biometric, knowledge based, etc
- Allows for secure shared use of mobile devices resulting in cost savings
- Flexible and scalable as an enterprise updates or diversifies its platforms

[10] https://www.dhs.gov/homeland-security-presidential-directive-12

[11] https://federalnewsnetwork.com/workforce/2021/01/new-normal-or-same-old-bureaucracy-feds-offer-mixed-views-on-telework-prospects-beyond-pandemic/

[12] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf

[13] https://www.yubico.com/works-with-yubikey/catalog/intellitrust-authentication-service/

[14] https://www.csoonline.com/article/3399858/phishing-attacks-that-bypass-2-factor-authentication-are-now-easier-to-execute.html

As agencies continue to facilitate and, in some cases, promote the use of mobile technology in virtualized work environments, YubiKeys provide the same level of authentication assurance to CISOs and ICAM managers that a PIV/CAC card provides at a workstation at the office. To solve these problems, some agencies have turned to derived credentials that can be embedded in mobile devices. When those services exist, they work well. But they are not by any means ubiquitous. Thankfully OMB M-19-17 allows for agencies to start piloting alternative authentication tools to be used to fill those gaps, and Yubico continues to deliver exceptionally well in those circumstances.

Use Case #2

Edge Cases – Contractors/Detailees/Seasonal Employees

Since HSPD 12 was issued, OMB has relied on the PIV card as its policy choice for strong authentication. After the OPM data breach in 2015, the Obama administration ran the Cybersecurity Sprint to issue PIV cards to the entire federal workforce – both privileged and unprivileged users. What those implementation efforts uncovered, however, was a series of “edge cases” that could not be secured through PIV issuance.

Contractors

Many of the contractors that supported federal departments and agencies were issued PIV cards and furnished with government devices. However, in most cases, government contractors work across multiple accounts (e.g., their government account, their company account, and sometimes their personal account). Additionally, there were several use cases in which government contractors could not receive a government-issued identity because of their status, the type of work they were performing, or their location (meaning the effort to provision a PIV card through in-person proofing was cumbersome and expensive).

YubiKeys can solve each of these cases while providing a range of authentication assurance commensurate with the duties of each contractor. First, YubiKeys can store up to 26 certificates and credentials on a single hardware token, allowing for security authentication across multiple accounts. Second, YubiKeys – through the use of FIDO authentication standards and remote/virtual proofing services – can provide the equivalent of AAL3 and IAL2 for any contractor. Finally, YubiKeys can work with almost any type of device or operating system through NFC, enabling secure authentication regardless of the type of working environment.

Detailees

Federal employees often move between agencies for varying periods of time while maintaining their home agency. These “details” to other agencies allow employees to grow in their careers or help solve difficult problems by leveraging their expertise. However, these stints at other agencies come with ICAM challenges and costs, given that the PIV card issued by one agency often does not work at another.

YubiKeys can easily solve these problems by storing the electronic certifications from multiple agencies on one hardware-based authenticator. Employees can easily move between workstations at their detailed agencies and their home agencies while saving money on the issuance of multiple PIV cards.

Seasonal Employees

There are many federal employees who are hired on a short-term, temporary basis. These employees may need to handle sensitive information, as in the case of the annual census, or they may need to access sensitive systems for a brief period of time. In both cases, it is important to have a high level of authentication assurance. However, the cost associated with provisioning a PIV card, even temporarily, becomes prohibitively expensive. According to the USAccess price sheet,[15] the price to issue a new card and maintain the certification for a year is $108.40. Annual certification maintenance alone is $41.40.

[15] https://www.fedidcard.gov/system/files/USAccess_Price_Sheet080119_Final.pdf

Issuing fully provisioned YubiKeys for less than the price of the PIV cards' annual certification maintenance can provide cost-effective security authentication solutions for seasonal work details across multiple periods of time. There is also the added benefit that – depending on the needs of the seasonal worker – a portable authenticator allows multiple employees to use the same mobile device, as in the case of a census worker collecting information with a tablet or phone.

Conclusion – Why Yubico?

Federal IT environments have changed dramatically in the past decade. Government agencies are migrating to cloud services and supporting an increasingly mobile workforce that carries multiple devices, not all of which are government furnished. The COVID-19 pandemic has accelerated this change, with agencies moving to support an increasingly remote workforce – a trend that is here to stay. The pandemic also magnified existing challenges, with PIV and CAC issuance made more difficult by nationwide enrollment office closures. The proliferation of mobile devices, which typically are not equipped with card readers, demonstrates the need for derived credentials and secure authenticators. The need for the government to move beyond PIV for authentication has never been greater.

While PKI-based PIV remains the underpinning of federal ICAM programs, updated OMB policy and NIST guidance are pushing the government toward more modern, risk-based authentication approaches that embrace Zero Trust architecture. Additionally, the recent EO requires federal agencies to resolve authentication challenges associated with their edge cases.

This changing environment and policy landscape provide an incredible opportunity for federal agencies to look for modern solutions to their authentication challenges as they build out their Zero Trust environments. Yubico's products offer an ease of use and compatibility that make it easy to weave into a federal agency's identity fabric. Also, Yubico's American manufacture of both its hardware and software adds an extra layer of assurance that its supply chain is secure from foreign influence and attack.

OMB M-19-17 paved the way for piloting the use of non-government-furnished authenticators that meet the security and privacy requirements of 800-63-3, and updates to NIST guidance are under way to account for their use. With the policy environment supportive of a more risk-based, cost-effective approach to security and identity, agencies can take advantage of an authentication solution that enables zero trust, virtual work, mobile-friendly architectures.

APPENDIX A: Federal ICAM Policy Response

Federal identity, credential, and access management (ICAM) policy has evolved significantly in the past decade, with updated policy and guidance pushing the government toward more modern, risk-based authentication approaches that embrace Zero Trust architecture. In the past four years alone, we have seen a new cybersecurity-focused executive order, updated Office of Management and Budget (OMB) guidance, and several publications from the National Institute of Standards and Technology (NIST). Combined, these efforts have responded to agency needs, market trends, and the evolving cybersecurity threat landscape. They also provide federal agencies with guidance, best practices, and, in some cases, mandates to modernize their ICAM approaches. Most recently, the new administration issued the above-mentioned executive order, drawing renewed focus to several critical cybersecurity areas mandating, among other things, federal agency adoption of multi-factor authentication (MFA) and implementation of Zero Trust architectures.[16]

Specifically, the executive order requires agencies to adopt multi-factor authentication to the "maximum extent" possible. To track progress, agencies must submit a report every 60 days to the Cybersecurity and Infrastructure Security Agency (CISA), OMB, and the National Security Council (NSC). At the end of 180 days, agencies that have not deployed MFA to the "maximum extent" must send a report to CISA, OMB, and the NSC detailing the reasons the agencies could not meet the timeline.

This requirement forces agencies to solve the more challenging authentication edge cases that are not traditionally solved by enterprise PIV card deployment. These edge cases have existed for years, in that there are a number of cases where someone accessing federal systems is either ineligible for a PIV card or cannot use their PIV card in a particular system or application.

This issue became especially acute after 2015, when the government made a huge push to deploy PIV cards in the wake of an Office of Personnel Management (OPM) data breach. While agencies made significant progress, the 15-20 percent of agency populations that could not take advantage of PIV cards to secure their systems have in many cases been relying on nothing more than usernames and passwords. Part of this is due to the fact that some parts of the government adopted a "PIV or nothing" approach – premised on the idea that since the PIV card is the "gold standard" when it comes to authentication, the government should not use other types of MFA. The unintended consequence of this approach was the persistence of weak password-based authentication solutions that created the potential for a potent attack by our adversaries.

While OMB opened the door to other potential approaches to MFA with OMB M-19-17, Enabling Mission Delivery Through Improved Identity, Credential, and Access Management,[17] most agencies have maintained their "PIV or nothing" approach to MFA.

This new executive order makes clear that "nothing" is no longer an acceptable option, and opens the door for agencies to use other MFA solutions, such as those based on the FIDO standards.

Providing flexibility in approaches to identity and authentication allows mission owners and authorizing officials to use a risk-based approach to identity and access management, especially in cases where there are no PIV cards issued.

There are several NIST publications that guide agencies in the identity space, including Federal Information Processing Standard (FIPS) 201-2 – *Personal Identity Verification*,[18] Special Publication 800-157, *Guidelines for*

[16] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[17] https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

[18] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

Derived PIV Credentials,[19] Special Publication 800-63-3, *Digital Identity Guidelines*,[20] and Special Publication 800-27, *Zero Trust Architecture*. While PKI-based PIV cards remain a core part of federal agency ICAM programs, the addition of NIST identity-related publications beyond PIV in the past 10 years demonstrates agencies' evolving identity needs. For example, FIPS 201-2 is currently undergoing revision to include expanding the set of PIV authenticators beyond the current set and beyond the smart card form factor.[21] As another example, SP 800-207 helps capture a cybersecurity concept and assist agencies in understanding how the Zero Trust principles or "paradigms" apply to the architecture issues; such guidance will be helpful as agencies address EO 14028 requirements to implement these architectures. Table 1 provides a summary of relevant NIST guidance.

Table 1: Relevant NIST Guidance

Title	Description
FIPS 201-2: Personal Identity Verification (August 2013) (undergoing revision)	This standard specifies the architecture and technical requirements for a common identification standard for federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and logical access to government information systems. The standard contains the minimum requirements for a federal personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive-12, including identity proofing, registration, and issuance. The standard also provides detailed specifications that will support technical interoperability among PIV systems of federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard.
SP 800-157: Derived PIV Credentials (December 2014)	This standard provides technical guidelines for the implementation of standards-based, secure, reliable, interoperable public key infrastructure (PKI)-based identity credentials that are issued by federal departments and agencies to individuals who possess and prove control over a valid PIV Card. The scope of this document includes requirements for initial issuance and maintenance of these credentials, certificate policies and cryptographic specifications, technical specifications for permitted cryptographic token types, and the command interfaces for the removable implementations of such cryptographic tokens.
SP 800-63-3: Digital Identity Guidelines (June 2017) (undergoing revision) **SP 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management (June 2017)**	The guidelines cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. They define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions. These guidelines focus on the authentication of subjects interacting with government systems over open networks, establishing that a given claimant is a subscriber who has previously been authenticated. The result of the authentication process may be used locally by the system performing the authentication or may be asserted elsewhere in a federated identity system. This document defines technical requirements for each of the three authenticator assurance levels.
SP 800-207: Zero Trust Architecture	Zero Trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A Zero Trust architecture (ZTA) uses Zero Trust principles to plan industrial and enterprise infrastructure and workflows. Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the Internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session on an enterprise resource is established. Zero Trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary. Zero Trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component of the security posture of the resource. This document contains an abstract definition of Zero Trust architecture and gives general deployment models and use cases where Zero Trust could improve an enterprise's overall information technology security posture.

Source: NIST publication abstracts

[19] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf

[20] https://pages.nist.gov/800-63-3/

[21] See https://www.nist.gov/topics/identity-access-management/roadmap-fips-201-personal-identity-verification-piv

About Venable’s Cybersecurity Services Team

Fully immersed in all aspects of digital identity and cybersecurity, Venable stands apart among law firms and consulting firms with its deep experience in standards, strategy, policy, and regulatory issues. Our team members draw on their past experiences working for and with various government and commercial entities in the privacy and technology landscape to provide solutions and insight into issues that impact our clients.

Our team has led policy development and implementation efforts at the White House National Security Council (NSC) and Office of Management and Budget (OMB), as well as in the Department of Defense, the National Institute of Standards and Technology (NIST), and the Department of Commerce. We participate in legislative advocacy, rulemakings, and development of new legal standards and advise organizations with regard to industry best practices and drafting codes of conduct and standards, helping them stay compliant with federal, state, international, and self-regulatory requirements. We leverage our long-standing relationships with government officials and industry stakeholders to ensure that our clients have the best support and are the first to know about movement on existing and future policies, regulations, and legislation that affect their businesses. Our knowledge, experience, and relationships make us uniquely suited to provide in-depth reporting on topics and issues within the industry.

Author Biographies

Jeremy A. Grant | Managing Director of Technology Business Strategy
Washington, DC | jagrant@Venable.com | +1 202.344.4646

As a member of Venable's Cybersecurity Risk Management Group, Jeremy Grant combines federal government and private sector experience to help clients develop growth strategies, identify and exploit market trends, and advise on policy impacts across the IT, cybersecurity, identity, and payments sectors. In this role, Jeremy utilizes his diverse background and deep understanding of business, technical, policy, and finance issues related to identity, privacy, and cybersecurity, having served in a range of leadership positions spanning government and industry.

Grant Schneider | Senior Director of Cybersecurity Services
Washington, DC | gmschneider@Venable.com | +1 202.344.4612

Grant Schneider is a recognized leader in the cybersecurity sector with extensive experience in driving organizational change, improving program maturity while reducing costs, developing policy and governance structures, and driving enterprise-wide technology modernization initiatives. Having served as the U.S. federal chief information security officer (CISO) based in the White House and on the White House National Security Council (NSC) as senior director for cybersecurity policy, Grant is uniquely positioned to assist clients in navigating the strategic, operational, and risk management needs of large-scale global technology environments.

Jamie M. Danker | Senior Director of Cybersecurity Services
Washington, DC | jmdanker@Venable.com | +1 202.344.8300

Jamie Danker combines her federal government and private sector experience to help clients build more trustworthy systems, products, and services through the adoption of cybersecurity and privacy risk management practices. Jamie brings deep privacy, identity, and cybersecurity knowledge, along with diverse perspectives from oversight, operational, and guidance organizations based on her prior roles in government and industry.

Ross B. Nodurft | Senior Director of Cybersecurity Services
Washington, DC | rbnodurft@Venable.com | +1 202.344.4403

Ross Nodurft counsels clients on issues related to risk management, government policy standards and regulatory compliance, and incident management. Having served as principal of Risk Management and Government Solutions at a digital identity and cybersecurity firm and chief of the Office of Management and Budget's (OMB) Cyber Team in the White House overseeing federal government cybersecurity policy and federal agency incident response, Ross has significant experience with advising clients on how to navigate issues at the nexus of homeland security, technology, and cybersecurity policy.

VENABLE LLP