PIV-I And Multifactor Authentication:
The Best Defense for Federal Government Contractors

Prepare Your Organization Now For Updated Federal Security Standards That May Affect Your Organization's Federal Contracts

This white paper explores...

- NIST SP 800-171 and why compliance is critical to federal government contractors, especially those that work with the Department of Defense
- Leveraging PIV-I credentialing with multifactor authentication as a defense against cyberattacks
- How PIV-I enables non-federal organizations to achieve security compliance

Introduction

In response to an unprecedented level of espionage and cyberattacks aimed at compromising critical government IT infrastructure—from networks to applications—the federal government last year announced new standards. Regulations have been enacted in 2016 to apply these standards to federal contractors and their subcontractors. The time to adopt is now.

As the type of cyber threats and targets continue to grow, many organizations are seeking a comprehensive solution aimed at eliminating weak links. The 2015 Office of Personnel Management (OPM) hack is one of the most significant cyber theft incidents in recent history. More recently, the reported Yahoo data breach announced September 22, 2016, affecting at least 500 million user accounts and believed by the company to have been perpetrated by a state-sponsored actor.

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 calls for "the protection of Controlled Unclassified Information (CUI) while residing in non-federal information systems and organizations." CUI is defined as "information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified."

Federal government contractors that handle "covered defense information" (CDI) under contract with the Department of Defense (DoD), one of the first agencies to implement NIST SP 800-171, face a compliance deadline of December 31, 2017.

The federal government recognizes that the protection of sensitive information--not just classified information--is paramount for its federal agencies to successfully accomplish their respective missions. Failure to properly secure sensitive data directly impacts the ability of the federal government to carry out important functions both inside and outside the federal IT environment.

A key standard under NIST SP 800-171 is multifactor authentication. This standard falls under section 3.5 of NIST SP 800-171, "Identification and Authen-

Cont.

tication," and represents one of the most substantial changes that will affect the greatest number of organizations. Beginning with DoD, the federal government no longer will allow simply a username and password to authenticate an individual's identity; rather, an organization must implement a multifactor paradigm, such as a username or PIN (something you know), a biometric marker such as a fingerprint (something you are), plus a smart card (something you have).

For non-federal organizations of any size that contract with the DoD, the requirements can be daunting. Significant organizational changes may be necessary, potentially requiring multiple vendors and additional managed services. As a result, the DoD is providing significant lead-time to organizations to update their internal security infrastructure and systems to become operational by December 31, 2017. Non-compliance could mean the loss of DoD contracts.

For non-federal organizations that work with other federal agencies outside of the DoD, a compliance deadline may not be far behind. The National Archives and Records Administration (NARA) on September 14, 2016 published a Final Rule that requires non-DoD federal contractors to implement the NIST SP 800-171 security controls. The rule takes effect November 17, 2016 and its provisions will begin showing up in the Federal Acquisition Regulation (FAR)—and federal contracts—after that. Thus, the multifactor authentication standard under NIST SP 800-171 is being extended beyond the DoD to other key federal agencies and their contractors.

Non-federal entities that handle CUI must begin the process to ensure multifactor authentication compliance, if they have not already done so, to ensure continued eligibility to compete for and win federal contracts.

PIV-I with Multifactor Authentication: The Gold Standard

In response to the multifactor authentication mandate, non-federal contractor organizations are scrambling to meet compliance. Several basic multifactor authentication frameworks exist such as soft tokens and hard tokens (e.g., smart cards, key fobs, or dongles) designed to store user credentials, and one-time passwords (OTP) sent to a mobile device.

However, none provide both the high assurance identity proofing and the robust physical-logical access—all within one single smart card—that is provided by the Personal Identity Verification (PIV) for federal entities and its counterpart for non-federal entities, Personal Identity Verification-Interoperable (PIV-I).

The PIV-I credential system supports robust identity proofing through the use of multifactor authentication, protecting against infiltration by even the most sophisticated hacking groups. A PIV-I credential is provisioned with digital certificates, photo and fingerprint and among the most effective ways of addressing security vulnerabilities both online and on-premise. A would-be hacker would have to infiltrate a given Public Key Infrastructure (PKI), and hack each individual card where the information is stored. Doing so would be practically impossible for a cyber espionage group physically located on the other side of the world. As a result, the PIV-I security framework, more than a decade in the making, has proven to be a win-win for federal agencies and non-federal entities. PIV-I works seamlessly across a wide range of physical and logical access control systems and provides additional flexibility to work through an innumerable set of scenarios.

PIV cards already are a necessary fact of life for federal agencies. Earlier this year Tony Scott, Chief Information Officer of the United States, said he wanted 100 percent use of PIV cards for privileged users of federal systems by the end of President Obama's term. And in June 2015, the Department of Veterans Affairs (VA) implemented a policy to make PIV cards mandatory on VA information systems, including those accessing the network with 'elevated privileges'.

Now, PIV-I cards are becoming a necessary fact of life for non-federal entities, especially those that handle CUI. PIV-I provides federal contractors with multifactor authentication for its employees while enabling them to check off one of the most significant hurdles to securing NIST SP 800-171 compliance.

PIV-I: A Single, Trusted Identity

The PIV-I framework features numerous advantages across a broad set of criteria:

Door to desktop: Typically in an enterprise environment a proximity badge is used for ID and physical access. For logical access, a username and password combination often represents the security token. In contrast, PIV-I provides a single, high-assurance identity credential that can be used to access everything from doors to desktops in a secure manner. The benefit of this is simpler access management, including swift revocation of compromised credentials plus full lifecycle identity management.

Platform agnostic: PIV-I provides a smooth transition across a diverse employee base to achieve the highest level of security. For example, the PIV-I credential can be trusted by any entity, either government or business, that accesses the Federal Bridge. By contrast, a construct like One Time Password (OTP) is often tied to a specific device, and although OTP can be agnostic for government or business, it does not have the same level of assurance.

Cryptographic data protection: PIV-I cards can facilitate a variety of important security measures within a single credential:

- Digitally sign documents (non-repudiation)
- Authenticate to networked resources
- Encrypt messages for communication
- Authenticate with an access control system that utilizes the same tool within well-defined standards—ensuring the solution will work with a myriad of technologies, from mainstream workstation and server operating systems to door readers and management systems that leverage cryptographic standards

Cyber awareness: The federal government has established specific standards for various levels of trust associated with different credential types, referred to as "Assurance Level." Federal policy sets forth four levels of assurance with level one being the lowest, requiring no identity verification — think of online email or commercial web sites allowing anonymous, unverified users to create accounts — and with level four representing the highest trust assurance possible. PIV-I credentials are considered Level of Assurance Four (LOA4) for the requirements of in-person identity proofing, hardware-based digital certificate storage and secure issuance policy to ensure the correct person receives the correct credential.

By providing each required user a physical credential, no matter what role they may play within the federal and non-federal CUI paradigm, the PIV-I credential reinforces the security-aware mindset required to ensure that data and access remain secure.

Strength and ubiquity: The PIV-I model more than offsets the initial investment in time and resources required to implement when invaluable data assets and information are on the line.

The damage wrought by high-profile hacks within the government and private sectors has shown the tremendous cost of insufficient security measures, casting new light upon the cost-benefit analysis of investing in the world's most robust security options. In short, federal contractors that handle CUI no longer can afford not to implement the multifactor authentication process PIV-I provides.

A derived credential: The nature of work and how it is conducted has continued to evolve. As workforces become more mobile and flexible—increasingly working remotely from a variety of geographical locations on a variety of devices—multifactor authentication that leverages a secure digital identity can greatly reduce the threat of cybersecurity breaches associated with remote access.

PIV-I can be utilized as a "derived credential," which is carried on mobile devices instead of a card. This option provides a cost-effective alternative to adding smart card readers to mobile devices or replacing machines that don't support the form factor. It also improves productivity, accommodating employees who prefer to use their personal mobile devices for work.

Credential Lifecycle Management: Through PIV-I, system administrators can check the status of any credential on their network. Coordinating refusal of access to a revoked credential can significantly reduce the lag time between identifying and refusing a compromised credential.

Mitigating the Cost of PIV-I

Organizations that implement PIV-I don't have to manage their own security infrastructure and hardware, including finding a Certification Authority (CA) for PKI setup, its own card management system and its own Identity Management System (IDMS), all of which pose significant setup, infrastructural and expertise costs. For organizations that need just a few cards or a few thousand, PIV-I capabilities can be acquired as a streamlined, out-of-the-box service—ready for an organization within a week as opposed to months.

PIV-I services can also be utilized in a cloud environment, providing scalability, redundancy, and then deployment and implementation. This allows the organization to scale its service requirements to match its current environment, adding additional PIV-I credentials on a per-credential basis.

Credential-based pricing makes the adoption affordable for organizations of all sizes by providing self-service pre-enrollment capabilities through a web portal and kiosks.

Conclusion

December 31, 2017 is quickly approaching. For those non-federal contractors that handle CUI—whether through a complex ecosystem with multiple levels of subcontractors and federal contracts, or those who need a handful of cards—the time to get ahead of NIST SP 800-171 is now.

With the above advantages in mind, full-service PIV-I credentialing represents a flexible, cost-effective and future-proofed method to achieve one of the most critical aspects of NIST SP 800-171 compliance. The cost of the assurance PIV-I provides an organization and its individuals far outweighs the costs of a major data breach.

To learn more about SureID, the leading provider of high-assurance identity solutions, visit: **www.sureid.com**