securityinformed.com
Making The World A Safer Place

Why Aren't The Federal Government's Physical Access Systems Compliant With HSPD-12?

Published on 17 Dec 2018

In the wake of 9/11, the Federal Government's secure-the-fort, big idea was to create an identity credential for all federal employees and contractors. Homeland Security Presidential Directive (HSPD)-12 set it all in motion. Today, we know the smartcard-based credential that arose from HSPD-12 as the Personal Identity Verification (PIV) card.

The PIV card is meant to give employees/contractors physical access to federal facilities and logical access to federal information systems. While using a PIV card for logical access has been largely successful and compliant with HSPD-12, implementing PIV-based, physical access control systems (PACS) has been much more difficult to conquer. As a result, HSPD-12 compliance for PACS has largely eluded the Federal Government. The noncompliance reasons are many, but there is now

hope for fully achieving HSPD-12's mandates.

Interoperability With Any Agency's PIV

> Beyond Passports, PIV cards represent the only other open-standards-based, multi-vendor-supported, identity credential program on the planet

All Executive Branch employees and long-term contractors, including the entire Department of Defense, have been issued PIV cards. This has been true since 2013. Beyond Passports, PIV cards represent the only other open-standards-based, multi-vendor-supported, identity credential program on the planet.

It seems so simple, where employees/contractors previously used their proximity card to open a federal facility door or go through a turnstile, they should now be able to use their PIV card. However, HSPD-12 took the PIV requirement one step further – compliant PACS must be interoperable with any agency's PIV. This introduced an entire magnitude of additional complexity.

A compliant, interoperable, PIV-based PACS should work like this: an authorized employee (or contractor) presents a PIV card (contact or contactless) to a card reader to enter whichever federal agency building they have reason to be. Over the last 14 years, in all but a very few cases, the lack of PACS' HSPD-12 compliance has prevented this from happening.

Secure Credential Policy

Today, less than 1% of the Federal Government's PACS are HSPD-12-compliant. At most federal facilities, especially those outside the National Capitol Region, a noncompliant PACS works like this: an authorized employee (or contractor) presents a proximity ('prox') badge to a proximity card reader to enter his or her agency's facility. At the fraction of federal facilities with upgraded PACS that work with PIV cards, virtually all such PACS fail to properly use a minimum number of PIV security features before granting access – let alone interoperate with a PIV card from any other agency.

> Active government solicitations are issued for new, non-compliant, proximity-based systems that perpetuate the delay to HSPD-12 compliance

New federal initiatives frequently suffer from having no policy to enforce their roll-out. That isn't the case with PACS compliance. Policies have been in place for so long that newer policies like Office of Management and Budget (OMB) M-11-11 (February 3, 2011) remind everyone what the policies said in 2004 and 2006. This year, OMB publicized its proposed OMB M-18-XX (Draft), which will replace M-11-11. OMB M-18-XX's (Draft) main PACS thrust is, once again, to ensure that everyone understands what the Federal Government's secure credential policy is. It hasn't changed since 2004.

It would be tempting to say that PACS technology isn't mature, but that isn't the case. In 2013, the Federal Government revamped the PACS portion of the FIPS 201 Evaluation Program and, since that time, all PACS on the General Services Administration's (GSA) Approved Products List are 100% compliant and interoperable. Yet, on any given day, active government solicitations are issued for new, non-compliant, proximity-based systems that perpetuate the delay to HSPD-12 compliance.

The usual suspects, policy and technology, are not the culprits for this epic delay.

Difficulties In Adopting HPSP-12 Compliance For PACS

- **Standards** – The Federal Government's approach to standards is to avoid a great deal of

specificity. It's an unspoken tenet that federal standards must be flexible, promote innovation and avoid disadvantaging any participating market segment. The opposite is true if your goal is interoperability: nearly every detail must be specified. Consider the standards-based success story of chip-based credit cards. When was the last time you used a credit card and it didn't work? Interoperability failures are nearly unheard of. If you look at the hundreds of volumes of technical specifications that cover minute aspects of every component in credit cards and payment terminals, you quickly realize why it works so well. Nothing is left to chance, nothing is a variable, and there is no optionality.

The Good News: Work to increase viability through deep scrutiny has progressed in recent years. The GSA APL PACS Testing Lab, set up in 2013, annually tests credentials from all PIV issuers against all GSA-approved PACS. This testing has significantly reduced interoperability failures at federal facilities.

- **Collaboration** – In the past, physical access practitioners from federal agencies rarely collaborated, unlike their logical access counterparts. This is also true for PACS procurement decision-makers across agencies and facilities.

***The Good News*: In 2018, an agency trend has emerged where finally physical access, physical security and IT practitioners have begun sitting down to discuss their shared responsibilities. We have already begun to see coordinated budget requests between IT and Security with enterprise architectures positioning PACS as an enterprise service on the network**

- **Scale** – The Federal Government owns so many buildings that they can't be counted. Google doesn't know how many there are and neither does any one government official.
- **Variability** – A significant percentage of facilities have unique aspects making a one-size-fits-all approach infeasible.

The Good News: Mature consulting services can now help agencies marry federal requirements

with their unique environments to develop robust PACS enterprise architectures. As we see this occurring more and more frequently, a repeatable, achievable, systems-based upgrade of all PACS may be on the horizon.

The GSA APL PACS Testing Lab annually tests credentials from all PIV issuers against all GSA-approved PACS

- **Provenance** – In many cases, different groups own different parts of a single facility, not all of whom might be subject to, or wish to interoperate with, a high-assurance compliant PACS. For example, GSA manages facilities for Legislative and Judicial tenants who aren't subject to HSPD-12. Policy dictates that GSA manage the PACS for the front doors of these facilities should be HSPD-12-compliant, despite the fact that these tenants likely don't have credentials that work with this technology. Sure, these tenants could commercially obtain a PIV-I credential, but almost none have.

- **Economics** – It's difficult for agencies to create their annual security budget requests when HPSD-12 PACS upgrades are in scope, because so many unknowns exist at each facility. To assess the cost, the time to complete, and the facility's existing equipment

inventory, it would be logical for an agency to hire a contractor with PACS expertise to perform a site assessment. Having to do capital planning for an assessment phase in advance of making the annual budget request for the PACS upgrade creates a never-ending cycle of delay. Especially at agencies with multi-year capital planning requirements. Many agencies, trying to avoid this delay cycle, have fallen prey to doing site assessments themselves. This results in their integrators doing their walk-throughs after the contract is awarded. This is the leading cause of PACS upgrade cost overruns.

- **Dependence on the agency's IT department** – Historically, PACS have been deployed on dedicated networks and are rarely ever connected to the enterprise, let alone the Internet. High-assurance PACS that validate credentials from other agencies must now communicate with many different systems on an enterprise network and over the Internet – so much so that the Federal Government reclassified PACS as IT systems.

The Good News: With collaboration increasing between Physical Security Officers (PSOs) and Chief Information Officer (CIOs), we expect this to improve in due course.

- **Resistance to change** – This is a classic human factors challenge, and it's a big one. PSOs have spent decades achieving their positions. PIV-based PACS could not be more different from the technologies that proceeded it, and such radical change is often resisted. When the value proposition is clear, change is adopted more readily. But security value isn't easily measured or observed. It is often said that the best performance review for a PSO is to note that nothing happened. And when something does happen, it is necessarily kept quiet so the risk can be remediated without calling attention to the vulnerability in the interim. To date, the value proposition of moving to PIV-based PACS has been entirely based on policy (without corresponding funding in most cases) and through the shock value of white hat hackers, showing how easily most proximity badges can be cloned. This is not the stuff of change agents.

PIV-based PACS could not be more different from the technologies that proceeded it, and such radical change is often resisted

Are These Challenges A Unique Situation?

No, these PACS challenges are not unique. Cybersecurity initially faced many of the same challenges that federal PACS face today. By 2000, the Federal Government recognized its urgent need to improve cybersecurity practices across its computing infrastructure and issued many policies that required agencies to improve. Improvement was sparse and inconsistent. GSA Schedules were set up to help agencies buy approved products and services to assist them, but this too produced lacklustre results.

> The Federal Government found that the best cybersecurity results occurred when enforced at the time an agency commissioned a system

Congress enacted the Federal Information Security Management Act of 2002 (FISMA) (now amended by the Federal Information Security Modernization Action of 2014). FISMA mandates an

Authority To Operate (ATO) accreditation process for all information systems. The Federal Government found that the best cybersecurity results occurred when enforced at the time an agency commissioned (vs. purchased) a system.

FISMA and ATO accreditation has been highly successful when implementing new systems. These cybersecurity requirements are the closest thing that the Federal Government has to the 'PIV Police' today. However, the PIV requirements in FISMA and ATOs currently apply to only logical access for information systems.

The proposed OMB M-18-XX (Draft) mentions that a FISMA PACS overlay to NIST SP 800-53 is forthcoming. The intent of the PACS overlay is to use the army of ATO accrediting officials in the Federal Government and enable them to assess implemented PACS as fit for purpose. This is the first time an enforcement approach has been brought forward that could reasonably succeed.

How Long For HSPD-12 Compliance?

We know that it won't take another 14 years to achieve HSPD-12 compliance. Pockets of compliance are popping up. Compliant procurements do exist, and the state of PACS across the Federal Government is better in 2018 than in any previous year. Progress to date has been at a constant rate. The question is: what would take for progress to occur at an exponential rate instead? A major attack or compromise involving PACS would certainly hasten upgrades, but let's hope that's not the solution.

> The energy distribution sector has been riding a wave of security upgrade demands to retrofit their facilities across the U.S.

The energy distribution sector, under nearly constant Advanced Persistent Threat attacks, has been riding a wave of security upgrade demands to retrofit their facilities across the U.S. The potential threat exists for Federal Government facilities as well.

Looking into the federal PACS-compliance crystal ball, we're beginning to see the faint outline of a

multi-faceted campaign of education, budgetary oversight and accreditation of PACS that will ultimately see us past the tipping point. Consider though, at the current rate of PACS enablement, a 50% compliance rate is still far in the future.

When that day arrives, the PIV card form factor may no longer be the key that fits that future lock. (Are you already using a mobile device's Bluetooth interface to open the door to your office building?) Taking decades to perform a technology upgrade is the aging elephant in the room no one talks about. By the time critical mass is achieved with an upgrade facing these many challenges, there are typically compelling reasons to start over again with the next generation of technology. That cycle may well prove to be the Federal Government's biggest PACS challenge of all.

Author Profile

Jeff Nigriny

You may also be interested in...

Unlocking Profits For Integrators In The Ever-Evolving World Of Access...

Whether you are a veteran in the access control world or have never installed a card reader before, there are always ways to increase profit...

Why Self-Service Kiosks Are A Target For Cyber Attacks

Today, customers are demanding immediacy, personalization and seamless services from their providers and our desire for instant gratificatio...

Shifting Focus: Internet Of Things (IoT) From The Security Manufacture...

The term Internet of Things (IoT) has almost been beaten to death at this point, as more and more security integrators, manufacturers and cu...