## PIV Cards Going Away? Not Quite. New OMB Memo Reaffirms and Expands Their Role!
## June 7, 2019

*by Sarbari Gupta*

On May 21, 2019, the Office of Management and Budget (OMB) released M-19-17, a policy memorandum entitled, “Enabling Mission Delivery through Improved Identity, Credential, and Access Management.” This far-reaching policy memo rescinds a number of significant previous memos in the area of identity management, including M-04-04 and M-11-11, and establishes a comprehensive roadmap for modernization of identity, credential and access management (ICAM) implementations within the federal executive branch.

M-19-17 (https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf) touches on the following significant points:

1. Emphasizes the importance of ICAM in securing the modern federal enterprise and protecting the privacy of citizens.
2. Recognizes that there have been tremendous developments in identity authentication and federation technologies and that government needs to move beyond the four discrete levels of identity assurance established by OMB Memo M-04-04.
3. Points to the latest release of NIST Special Publication 800-63-3 as a path forward for considering new technologies for identity authentication and federation as a part of a broader digital risk management model.
4. **Confirms that Homeland Security Presidential Directive 12 (HSPD-12** (https://www.dhs.gov/homeland-security-presidential-directive-12)**) and the latest version of Federal Information Processing Standard 201 (FIPS 201** (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf)**) remain the government-wide policy and standard for common identification of federal employees and contractors and promotes more effective and efficient use of the huge investment already made in issuing Personal Identity Verification (PIV) credentials to all federal enterprise identities.**
5. Encourages agencies to pilot other authentication solutions that align with the spirit of HSPD-12 for the purpose of informing updates to the related NIST standards and technical guidelines.
6. Establishes a clear set of objectives for federal agencies to harmonize their ICAM modernization efforts through specific governance, architecture and acquisition efforts.
7. Provides a clear mandate that agencies need to minimize and protect citizens’ personal information by promoting reuse of existing identity credentials issued to citizens, and minimize the burden on citizens who access federal services by sharing identity proofing information across agencies.
8. Enumerates a set of responsibilities and actions for agencies that lead the standardization and execution of government-wide ICAM efforts.

While all of the above points are important, I would like to focus on #4. The memo makes it clear that FIPS 201 is still the government-wide standard for common identification and that agencies need to leverage the existing investment made in PIV cards through several distinct paths:

- Continue to issue and manage PIV cards in accordance with Office of Personnel Management requirements. No changes here.
- Require use of PIV cards as the primary means of identification and authentication for federal enterprise users' access to federal information systems and federally-controlled physical facilities. While most agencies have implemented PIV-based logical access, many have yet to implement PIV-based physical access. This memo requires that agencies use PIV-based authentication for physical as well as logical access.
- Enable the acceptance of Derived PIV credentials (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf) by applications and devices. While a small set of agencies have started to pilot and implement Derived PIV credentials, most have not. This memo emphasizes that agencies need to embrace Derived PIV credentials for authentication using mobile platforms.
- Identify and resolve barriers to the acceptance and use of PIV credentials issued by other government agencies to promote cross-government identity federation and interoperability. Today, federal enterprise users who support multiple agencies (such as contractors) have to go through an elaborate and expensive process to obtain a PIV card from each agency supported. This is true despite the fact that:
    - FIPS 201 specifies a common set of identity proofing, registration and issuance requirements for PIV cards.
    - There is a common PKI trust infrastructure – the Federal Common Policy Certification Authority (CA) and Federal Bridge CA – to accept the PIV credentials.
    - NIST Special Publication 800-73 provides the card architecture and interface specifications to facilitate technical interoperability between PIV systems.

If agencies were to accept PIV cards issued by other agencies for authentication of users who need physical or logical access, it would represent a huge step forward in achieving HSPD-12's vision of a common identification standard that helps to "increase government efficiency."

- Require and use PIV credential digital signature capability. Agencies have already invested in implementing PIV digital signature credentials on their PIV cards. However, few agencies have rolled out an appropriate level of use of the digital signature capability among users. If implemented properly, more pervasive use of digital signatures by federal enterprise users would significantly improve the assurance level of information exchanges and communications and prevent identity spoofing and phishing attacks.
- Protect confidentiality of data shared between two or more federal enterprise users by applying encryption capability of PIV credentials. Agencies are already issuing PIV cards with PIV encryption credentials. However, most agencies have not rolled out PIV encryption in their environments for a variety of reasons. Again, appropriate use of PIV encryption would significantly improve the confidentiality of information exchange among federal enterprise users.

In summary, it is worth pointing out that OMB M-19-17 firmly reinforces and expands on prior policies related to HSPD-12 and use of FIPS 201 as the common identity standard. M-19-17 also opens the door for considering and piloting alternate forms of identity authenticators that can meet the intent of HSPD-12 so that the lessons learned can be used to inform the evolution of NIST ICAM standards.

OMB should be applauded on the release of this sweeping and comprehensive policy memo. It will surely strengthen and modernize ICAM implementations within the government.

*Sarbari Gupta is the President and CEO of Electrosoft and an identity management geek! She is a named co-author of NIST SP 800-63-2 and NIST SP 800-157 and a significant contributor on the original FIPS 201 standard.*

**RETURN TO ELECTROBLOG (/ELECTROBLOG)** SHARE (HTTPS://WWW.LINKEDIN.COM/CWS/SHARE?URL=HTTP://WWW.ELECTROSOFT-INC.COM/RESOURCES/PIV-CARDS-GOING-AWAY-NOT-QUITE-NEW-OMB-MEMO-

REAFFIRMS-AND-EXPANDS-THEIR-ROLE)

## WE ARE HIRING

### Join Our Team

At Electrosoft we pride ourselves on the dynamic projects we deliver - challenge yourself and join our team!

**JOIN OUR TEAM (/CAREERS)**

## OUR TALENT NETWORK

### Our Talent Network

Electrosoft is always adding new opportunities. Join our Talent Network and let your next career opportunity find you.

**JOIN OUR TALENT NETWORK (HTTPS://ELECTROSOFT-INC.CLEARCOMPANY.COM/CAREERS/JOBS/BCB1A4CD-E51B-A58E-C84D-E061B3D671FF/APPLY?SOURCE=1085553-CJB-0)**

## LOCATION

Corporate Headquarters
1893 Metro Center Drive Suite #228
Reston, VA 20190

**CONTACT US (/CONTACT-US)**

## CERTIFICATIONS

## FOLLOW US