May 6, 2018

The Honorable Mick Mulvaney
Director
Office of Management and Budget (OMB)
1725 17th Street N.W.
Washington, D.C. 20502

Re: Comments on draft OMB Identity Policy M-18-XX: *Strengthening the Cybersecurity of Federal Agencies through Improved Identity, Credential, and Access Management*

Dear Director Mulvaney:

I am writing on behalf of the Security Industry Association (SIA), which is comprised of more than 800 member companies that develop, manufacture and integrate security products and services.

We appreciate the opportunity to offer the following comments on the draft identity policy, prepared jointly by the SIA Identity and Procurement Policy Working Groups. These member companies provide technology products in the areas of cybersecurity, logical and physical access control, and other types of security systems that are crucial to protecting U.S. government facilities and personnel around the world. For many years SIA and its members have provided input and guidance to federal agencies and the U.S. Congress concerning implementation of Homeland Security Presidential Directive 12 (HSPD-12)*, Policy for a Common Identification Standard for Federal Employees and Contractors*, which is foundational to federal Identity, Credential, and Access Management (ICAM) initiatives.

Summary

We support the draft policy's consolidation of disparate guidance to agencies to provide a more cohesive and coherent approach to ICAM governance, adoption and modernization, and adoption of NIST SP 800-63, *Digital Identity Guidelines* as normative for the federal government.

The draft policy includes instructions to agencies addressing the wide spectrum of cases where ICAM is applicable. However, we believe the provisions related to federal physical access control systems (PACS) are particularly important, as PACS are crucial to cybersecurity protections both as information systems and as a critical element of facility security.[1]

The issuance of personal identity verification (PIV) credentials across the federal government for employee network access is nearly complete, as logical access control solutions have been widely deployed in recent years. Yet for physical access, PACS at a majority of federal facilities require significant changes to achieve implementations fully compliant with Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors,*[2] utilizing authentication mechanisms that offer extremely low assurance levels, leaving significant physical and cybersecurity risks unaddressed.

The draft policy would strengthen PACS modernization and compliance efforts by requiring that agencies engage in more coordinated, multidisciplinary efforts to carry out ICAM strategies, as well as calling for a PACS-specific overlay of applicable security and privacy controls to ensure complaint implementation. The policy would be even stronger if it

[1] See attached SIA Revisions Table
[2] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

included timelines required for achievement of related tasks directed to specific agencies and for general agency compliance, much like the timelines included in OMB M-11-11 that is superseded by the policy.

Modernization of federal PACS is essential to achieving the goals of ICAM and addressing a range of homeland and national security threats across the counterterrorism, counterintelligence and cyber fronts. Further, the full application of Continuous Diagnostic Monitoring (CDM) – a major cybersecurity priority in the draft policy – requires FIPS 201 complaint PACS to fulfill Phase 3 implementation.

For these reasons, we believe that in order for the new policy to be successfully implemented, federal IT modernization efforts and funding must prioritize achieving FIPS 201 compliant PACS implementations across the federal government.

The additional comments below follow the draft memo outline sequentially, while suggested revisions to the text are provided in the attached spreadsheet for your convenience.

Government-wide Responsibilities

As mentioned above, the General Services Administration (GSA) is instructed, along with NIST, OPM and DHS develop a security and privacy control "overlay" specifically applicable to PACS. This should provide a means for ensuring that an agency's equipment and its configuration are compliant with FIPS 201 and other relevant standards. We believe this essential to increasing compliance moving forward, and that it must be verified by authorizing officials at the point of implementation to be effective.

GSA is also directed to continue to manage the FIPS 201 evaluation program and Approved Products List (APL) to provide compliant and interoperable solutions for logical and physical access control. We strongly support the retention of the administration of this program within GSA, as well as related personnel with specialized expertise. This is especially important given the central and expanded roles for the evaluation program articulated in the draft policy.

The U.S. Department of Homeland Security (DHS) is directed to update the *Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*, and other pertinent Interagency Security Committee (ISC) guidance, to ensure they are "aligned with government-wide policy for the implementation of PIV credentials." We understand current physical security countermeasures guidance to facility security personnel under this standard needs to be updated to fully include provisions relevant to FIPS 201 compliant PACS, so this change is crucial to achieving the goals of the draft policy.

Attachment: Foundational ICAM Requirements

Federal Employees and Contractors

The issuance of this new guidance is an opportunity to clarify the applicability of Personal Identity Verification-Interoperable (PIV-I) credentials. PIV and PIV-I credentials are fully interoperable in both form and function but are issued to different groups. PIV credentials are issued for federal employees and certain long-term contractors, and PIV-I for other contractors as well as legislative and judicial branch employees, state and local government employees and others the executive branch needs to interact with in ways that require trusted authentication to access facilities and networks within the federal enterprise.

The PIV-I credential is issued using the same rigorous identity proofing model, contains digital certificates binding the identity cryptographically that are issued under the same high security provisions, and uses a smart card form factor that not only meets the security and operational requirements, but is used by PIV issuing organizations.

However, there is a misconception that because a federal suitability background investigation has not been performed and adjudicated as a condition of PIV-I issuance, the PIV-I credential is fundamentally weaker than the PIV credential.

The difference is that for PIV-I, while a federal background check occurs after issuance, it is still a condition of authorization prior to a PIV-I holder accessing a federal facility or network. The results are linked to the PIV-I credential and become part of an attribute database for future reference.

The absence of the background investigation at issuance does not invalidate or weaken the assurance of identity provided by the PIV-I identity proofing process or the binding of identity to the credential. And importantly, mere possession of a PIV or PIV-I credential is not sufficient to authorize access, which requires the validation of additional criteria.

Greater reliance on PIV-I credentials provides a security benefit. Issuing PIV credentials to non-Federal employees forces the federal government to create a pseudo-employer relationship with the credential bearers. But the government will not be the first to know if a contractor leaves employment with his sponsoring organization, introducing a risk that the individual's federally issued PIV will not be revoked in a timely manner.

In partnership with OPM for background investigations, and in concert with FIPS 201-2, which establishes the chain of trust to transfer identity records between agencies, it would be more cost effective, efficient, and ultimately more secure to fully leverage the PIV-I credential in a contract employee's possession as the basis for identity, rather than to go through the exercise of issuing a PIV credential.

For these reasons, we recommend that the draft policy clarify that PIV-I credentials can be utilized in lieu of a PIV credential as long as the required background check has been successfully performed (see attached SIA revisions table).

Physical Access Control Requirements

Agencies are directed to ensure the "use of the PIV credential for physical access to Federal buildings are implemented in accordance with…" NIST SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS).* The revision of this document, which has been in draft form for more than a year, must be finalized by the time the new policy goes into effect in order truly help strengthen agency ICAM implementation. Correcting this will result in accurate guidance and overall enforcement.

The current version of NIST SP 800-116 is out of date and conflicts with other HSPD-12 driven requirements. For example, it allows and recommends implementations that are not acceptable under FIPS 201. We recommend that NIST SP 800-116 be updated with the past recommendations of the Security Industry Association (and other industry groups), which have been collected on multiple occasions by NIST, but never released.

Endnotes

Endnote #12 states "GSA maintains a Special Item Number (SIN) on Information Technology (IT) Schedule 70 for the acquisition of approved HSPD-12 Implementation Products and Services. All logical and physical access control products and services provided via GSA acquisition vehicles shall be included on Schedule 70."

Requiring all logical access control (LACS) and PACS provided through GSA to be listed on Schedule 70 is unnecessary to the purpose and goals of the draft policy and contradicts current practice, as products listed on the GSA FIPS 201 Approved Products List (APL) and services meeting the requirements of the GSA FIPS 201 Evaluation Program are on more than one schedule.[3] Many contractors under both IT Schedule 70 and Schedule 84 (law enforcement and security products) SINS meet these requirements and are currently providing such products and services to the government. For this reason, we recommend eliminating this endnote (see attached SIA revisions table).

In 2016, Schedule 84 added two new SINS specifically for PACS, 246-35-7 and 246-60-5, which include only FIPS 201-compliant products and services, in order to provide customers with a better way to identify these products. Agencies are accustomed to utilizing Schedule 84 or Schedule 70 for PACS, often depending on the type of products and services

[3] https://www.idmanagement.gov/buy/

required, as elements of a complete PACS system extend beyond IT components in architecture, function, and implementation. Related elements include locks, card readers, keypads, control panels, door contacts, controllers and exit devices, as well as integration with fire alarm, intrusion detection and other security systems. The government has already provided agencies with authoritative sources of related acquisition information including GSA's *PACS Ordering Guide*[4] and *www.idmanagement.gov*, which further explains these options and requirements.

In referencing HSPD-12 policy, standards and guidelines, endnote #20 refers to OMB M-05-24, NIST FIPS 201, and NIST SP 800-series guidelines related to PIV issuance, use, and management, as well as the OPM Federal Investigative Standards and OPM Credentialing Standards. Again, here it should be clarified that PIV-I credentials could be utilized in lieu of a PIV credential as long as the required background check has been successfully performed (see attached SIA revisions table).

We appreciate the opportunity to offer these comments, as well as your consideration. Please let us know if SIA or our members can be of any further assistance to you. Thank you for your leadership in efforts to improve cybersecurity through strengthening federal ICAM programs and initiatives.

Sincerely,

Don Erickson

Don Erickson
CEO
Security Industry Association
8405 Colesville Road, Suite 500
Silver Spring, MD 20910
derickson@securityindustry.org
301-804-4700

[4] https://www.gsa.gov/cdnstatic/Guide_to_PACS_-_REVISED_060717.pdf

Table of Suggested Revisions Accompanying SIA Comments on Draft OMB Memorandum

M-18-XX: Strengthening the Cybersecurity of Federal Agencies through Improved Identity, Credential, and Access Management

#	Section	M-18-XX text	Suggested Revision	Explanation
1	Intro paragraph	"Agencies must be able to identify, credential, monitor, and manage user access to information and information systems across their enterprise in order to ensure secure and efficient operations."	"Agencies must be able to identify, credential, monitor, and manage user access to information, information systems, **secured areas and facilities** across their enterprise in order to ensure secure and efficient operations."	Requirements under ICAM and HSPD-12, apply to both logical and physical access control.
2	Attachment: Foundational ICAM Requirements Federal Employees and Contractors	Employees and contractors who require long-term[19] access to Federally-controlled facilities or Federal information systems fall under the scope of Homeland Security Presidential Directive-12 and shall be issued a PIV credential in accordance with relevant policy, standards and guidelines.[20] Agencies should refer to OMB M-05-24 for additional HSPD-12 applicability requirements.[21]	Employees and contractors who require long-term[19] access to Federally-controlled facilities or Federal information systems fall under the scope of Homeland Security Presidential Directive-12 and shall be issued a PIV credential in accordance with relevant policy, standards and guidelines.[20] **However, existing valid PIV-I credentials in the possession of contractor personnel may be leveraged in lieu of the issuance of a PIV provided the requisite background investigation has been completed and adjudicated successfully.** Agencies should refer to OMB M-05-24 for additional HSPD-12 applicability requirements.[21]	There is a misconception that because a federal suitability background investigation has not been performed and adjudicated as a condition of PIV-I issuance, the PIV-I credential is fundamentally weaker than the PIV credential. The difference is that for PIV-I, while a federal background check occurs after issuance, it is still a condition of authorization prior to a PIV-I holder accessing a federal facility or network. The results are linked to the PIV-I credential and become part of an attribute database for future reference. The absence of the background investigation at issuance does not invalidate or weaken the assurance of identity provided by the PIV-I identity proofing process or the binding of identity to the credential. And importantly, mere possession of a PIV or PIV-I credential is not sufficient to authorize access, which requires the validation of additional criteria.

3	Attachment: Foundational ICAM Requirements Credential Use	PIV credentials shall be used as the standard means of authentication for Federal employee and contractor access to Federal information systems.[24] All systems under development shall be enabled to integrate with PIV credentials, in accordance with NIST guidelines, prior to being made operational. Additionally, when procuring services or upgrading existing systems, agencies shall require that these services or systems be enabled to use PIV credentials for authentication.[25]	PIV credentials shall be used as the standard means of authentication for Federal employee and contractor access to Federal information systems.[24] All **logical access and physical access control** systems under development **by any Executive Branch agency** shall be enabled to integrate with PIV credentials, in accordance with NIST guidelines, prior to being made operational. Additionally, when procuring services or upgrading existing systems, agencies shall require that these services or systems be enabled to use PIV credentials for authentication.[25]	This section should specify what type of systems and which agencies are subject to the requirement, as not all are.
4	Endnote #12	GSA maintains a Special Item Number (SIN) on Information Technology (IT) Schedule 70 for the acquisition of approved HSPD-12 Implementation Products and Services. All logical and physical access control products and services provided via GSA acquisition vehicles shall be included on Schedule 70.	**delete endnote #12**	Requiring all logical access control (LACS) and PACS provided through GSA to be listed on Schedule 70 is unnecessary to the purpose and goals of the draft policy and contradicts current practice, as products listed on the GSA FIPS 201 Approved Products List (APL) and services meeting the requirements of the GSA FIPS 201 Evaluation Program are on more than one schedule.[5] Many contractors under both IT Schedule 70 and Schedule 84 (law enforcement and security products) SINS meet these requirements and are currently providing such products and services to the government. For this reason, we recommend eliminating this endnote.

[5] https://www.idmanagement.gov/buy/

5	Endnote #20	Refer to OMB M-05-24, NIST FIPS 201, and NIST SP 800-series guidelines related to PIV issuance, use, and management, as well as the OPM Federal Investigative Standards and OPM Credentialing Standards.	Refer to OMB M-05-24, NIST FIPS 201, and NIST SP 800-series guidelines related to PIV issuance, use, and management, as well as the OPM Federal Investigative Standards and OPM Credentialing Standards. **PIV-I credentials in the possession of contractors may be utilized in lieu of a PIV credential provided the requisite background check has been successfully adjudicated.**	Aligns with suggested revision #2 above.