EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

May 21, 2019

M-19-17

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought
Acting Director

SUBJECT: Enabling Mission Delivery through Improved Identity, Credential, and Access Management

This memorandum sets forth the Federal Government's[1] Identity, Credential, and Access Management (ICAM) policy and includes the following sections:

I. Contextualizing Identity in the Federal Government
II. Managing Identities, Credentials, and Access in Modern Government
III. Adapting the Government's Approach to Homeland Security Presidential Directive 12 (HSPD-12)
IV. Shifting the Operating Model beyond the Perimeter
V. Improving Digital Interactions with the American Public
VI. Enumerating Government-wide Responsibilities

I. Contextualizing Identity in the Federal Government

For the purposes of this policy, "identity" refers to the unique representation of a subject, for example, a person, a device, a non-person entity (NPE), or an automated technology, that is engaged in a transaction involving at least one Federal subject or a Federal resource, for example, Federal information, a Federal information system,[2] or a Federal facility or secured area. This policy may refer to identity in two contexts: (1) Federal enterprise identity or (2) public identity. Federal enterprise identity, or, simply, enterprise identity, refers to the unique representation of an employee, a contractor, an enterprise user, such as a mission or business partner, a device, or a technology that a Federal agency manages to achieve its mission and business objectives. Public identity refers to the unique representation of a subject that a Federal agency interacts with, but does not directly manage, in order to achieve its mission and business objectives. Public identity may also refer to a mechanism of trust used to render services to the American public.

[1] This memorandum is not applicable to national security systems (NSS) as defined in 44 U.S.C. § 3552 (Federal Information Security Modernization Act of 2014), although OMB encourages owners and operators of NSS to utilize the requirements in this document where appropriate.

[2] Pursuant to OMB Circular A-130, "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

II. Managing Identities, Credentials, and Access in Modern Government

Advances in technology have enabled more digital interactions and business transactions, offering the Federal Government an opportunity for faster, more reliable connections and operations. In conjunction with this opportunity, however, a new set of challenges has emerged, because information about individuals has become more widely available through social media and breaches of personally identifiable information (PII).[3] In favor of this opportunity, the Federal Government continues to refresh its digital infrastructure through comprehensive efforts focused on cybersecurity, procurement, and management of a workforce capable of operating modern, frequently cloud-based environments. To address the challenges that have emerged alongside this opportunity, embedded within these efforts is an intensified focus on risk management and the adoption of processes, policies, and solutions that enhance privacy and security and that mitigate the degradation of operational service delivery. Accordingly, identity management has become even more critical to the Federal Government's successful delivery of mission and business promises to the American public. As such, through this Federal ICAM policy, the Government is enacting a common vision for identity as an enabler of mission delivery, trust, and safety of the Nation.

To ensure secure and efficient operations, agencies of the Federal Government must be able to identify, credential, monitor, and manage subjects that access Federal resources, including information, information systems, facilities, and secured areas across their respective enterprises. In particular, how agencies conduct identity proofing, establish enterprise digital identities, and adopt sound processes for authentication and access control significantly affects the security and delivery of their services, as well as individuals' privacy. [4]

Furthermore, in line with the Federal Government's updated approach to modernization, it is essential that agencies' ICAM strategies and solutions shift from the obsolete Levels of Assurance (LOA)[5] model towards a new model informed by risk management perspectives, the Federal resource accessed, and outcomes aligned to agency missions. To set the foundation for identity management and its usage to access physical and digital resources, agencies must implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3 and any successive versions (hereafter referred to as NIST SP 800-63). While NIST SP 800-63 is the foundation for digital identity, agencies must use it in combination with the remaining suite of publications that relate to identity management issued by NIST, the Office of

---

[3] Per OMB Circular A-130, "Personally Identifiable Information" means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

[4] For definitions of terms such as digital identity, identity proofing, federation, and credential, see NIST Special Publication (SP) 800-63-3, *Digital Identity Guidelines* (or any successive version) available at http://csrc.nist.gov/publications.

[5] The concept of LOA as a single ordinal that drives implementation-specific requirement is retired. Rather, the updates to NIST 800-63-3 combine appropriate business and privacy risk management with mission need, and separate the individual elements of identity assurance into discrete, component parts.

Personnel Management (OPM), and the Department of Homeland Security (DHS) to form a comprehensive approach to identity proofing that safeguards privacy and security.[6]

III. Adapting the Government's Approach to Homeland Security Presidential Directive 12 (HSPD-12)

HSPD-12 remains the Government-wide policy for the promulgation of standards-based, secure, and reliable forms of identification issued by the Federal Government to its employees, contractors, and other enterprise users. Additionally, Federal Information Processing Standard (FIPS) 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors* (or successive version),[7] remains the Government-wide standard for common identification, as called for by HSPD-12. In accordance with this standard, NIST guidelines, and Office of Personnel Management (OPM) requirements, a PIV credential is the aggregate output of the processes used for identity proofing, vetting, and authoritatively binding the identity of a human credential holder to an authenticator. However, as technology evolves, the Government must offer flexible solutions to meet changing technology needs and shift the focus from managing the lifecycle of credentials to the lifecycle of identities.

1. Agencies shall follow the requirements issued by OPM regarding the eligibility to issue, suspend, and revoke PIV credentials.[8]

2. Agencies shall require PIV credentials (where applicable in accordance with OPM requirements) as the primary means of identification and authentication to Federal information systems and Federally controlled facilities and secured areas by Federal employees and contractors.

    - Agencies shall use Derived PIV Credentials[9] for Federal employees, contractors, and other enterprise users (where applicable in accordance with OPM requirements) and to enable the acceptance of Derived PIV Credentials by applications and devices.

---

[6] A comprehensive list of identity publications is available at https://www.idmanagement.gov/.

[7] FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors* (or any successive version) is available at https://csrc.nist.gov/publications.

[8] OPM is designated the Suitability and Credentialing Executive Agent in Executive Order 13764 Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters https://www.Federalregister.gov/documents/2017/01/23/2017-01623/amending-the-civil-service-rules-executive-order-13488-and-executive-order-13467-to-modernize-the.

[9] NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials (or any successive version or replacement guidelines) is available at https://csrc.nist.gov/publications.

- Agencies shall work with the Federal CIO Council, the Federal Privacy Council, and NIST to pilot[10] additional solutions (e.g., different authenticators) that meet the intent of HSPD-12 and advance the technical approach to managing identities. The output of these pilots will drive improvements to NIST guidelines and Government-wide ICAM requirements including areas such as mobile and cloud identity.

- Agencies shall implement processes to manage access control, including the ability to revoke access privileges, when no longer authorized, and to revoke or destroy credentials in a timely manner. This is necessary to prevent unauthorized access to information systems when the employee or contractor separates from the agency, or the credential has been lost. Additionally, this serves to mitigate insider threats associated with compromised or potentially compromised credentials.

- Agencies shall ensure that use of the PIV credential for physical access to Federal facilities and secured areas is implemented in accordance with *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (or any successive version)[11] and NIST SP 800-116 R1, *Guidelines for the Use of PIV Credentials in Facility Access* (or any successive version).[12]

3. Agencies, in collaboration with OMB as necessary, shall support cross-government identity federation and interoperability by identifying and resolving obstacles to accepting the PIV identity assertions from other agencies to grant access (where authorized) to agency information systems, facilities, and secured areas. This includes:

    - Implementing processes for the electronic verification of PIV identity assertions from other agencies.

    - Accepting and leveraging existing, valid PIV credentials, including those issued by other agencies and electronically verified, rather than issuing new ones. This is equally applicable for logical and physical access (where authorized).

---

[10] Information on the process for requesting pilots is available at https://www.cio.gov/.

[11] *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* defines the criteria and processes that those responsible for the security of a facility should use to determine its facility security level, and provides an integrated, single source of physical security countermeasures. The guidance is available at https://www.dhs.gov/publications.

[12] NIST 800 116 R1 (or any successive version) contains guidance on the use of PIV credentials in physical access control systems (PACS). PACS are information systems, and they include, for example, servers, databases, workstations, and network appliances in either shared or isolated networks. The guidance is available at https://csrc.nist.gov/publications.

- Establishing and maintaining agreements (where required) to facilitate cross-government identity federation.

4. Agencies shall establish capabilities aligned to Federal ICAM Architecture and Continuous Diagnostics and Mitigation (CDM)[13] requirements that enable the continuous vetting and evaluation of fitness of personnel subject to HSPD-12.

    - These capabilities will strengthen the Federal Government's approach to make risk-adaptive decisions regarding access to information systems, facilities, and secured areas as intended by HSPD-12.

5. Agencies shall require and implement the use of the PIV credential digital signature capability. For individuals that fall outside the scope of PIV applicability, agencies should define and leverage credentials when using digital signatures.

6. Agencies should use PIV credentials as a method to encrypt information in transit and shared between two or more Federal employees or contractors.

IV. Shifting the Operating Model beyond the Perimeter

The interwoven technical architecture of the Federal Government creates complexity in managing access to resources, safeguarding networks, and protecting information. While hardening the perimeter is important, agencies must shift from simply managing access inside and outside of the perimeter to using identity as the underpinning for managing the risk posed by attempts to access Federal resources made by users and information systems. To ignite adoption of this new mindset around ICAM capability deployment across the Federal Government, each agency must harmonize its enterprise-wide approach to governance, architecture, and acquisition.

Governance

1. Each agency shall designate an integrated agency-wide ICAM office, team, or other governance structure[14] in support of its Enterprise Risk Management capability to effectively govern and enforce ICAM efforts.

---

[13] The CDM program enhances the overall security and privacy posture of the Federal government by providing Federal agencies with capabilities to reduce the attack surface of their respective networks, identify cybersecurity risks, and enable agencies to prioritize actions to mitigate or accept risks based on the potential impacts to their missions. CDM accomplishes this by working with agencies to deploy tools on agency networks that provide enterprise-wide visibility of what assets, users, and activities are on their networks. This actionable information allows agencies to effectively monitor, defend, and rapidly respond to cyber incidents. Information on CDM is available at https://www.dhs.gov/cdm.

[14] Examples of ICAM governance structures is available at https://www.idmanagement.gov/.

- This structure should include personnel from the offices of the Chief Information Officer, Chief Financial Officer, Human Resources, General Counsel, Chief Information Security Officer, Senior Agency Official for Privacy, Chief Acquisition Officer, Senior Official(s) responsible for Physical Security, and component organizations that manage ICAM programs and capabilities, including ICAM capabilities deployed through the CDM Program.

- Chief Operating Officers (COOs)[15] or the agency equivalent role shall ensure that there is regular coordination among agency leaders and mission owners to implement, manage, and maintain the agency's ICAM policies, processes, and technologies.

- While the agency governance structure described above will facilitate oversight of the implementation of Government-wide and agency enterprise-specific requirements, all bureaus, components, and other organizations at the sub-enterprise level must support efforts to harmonize ICAM across their respective agency by adhering to requirements and fostering accountability at all levels of the organization.

2. Each agency shall define and maintain a single comprehensive ICAM policy, process, and technology solution roadmap, consistent with agency authorities and operational mission needs. These items should encompass the agency's entire enterprise, align with the Government-wide Federal Identity, Credential, and Access Management (FICAM) Architecture and CDM requirements, incorporate applicable Federal policies, standards, playbooks, and guidelines, and include roles and responsibilities for all users.[16]

3. Each agency shall outline agency-wide performance expectations for security and privacy risk management throughout the identity lifecycle. These performance expectations shall support Government-wide management requirements, such as the President's Management Agenda (PMA) Cross Agency Priority (CAP) goals.

    - Agencies shall incorporate objectives for improving ICAM into their strategic plans and review their progress with OMB as part of their strategic reviews.[17]

---

[15] Per M-18-19, the COO is responsible for providing overall organization management to improve and achieve the mission and goals of the agency. COOs provide organizational leadership to improve performance of both mission and management functions. For more information, refer to https://www.whitehouse.gov/omb/information-for-agencies/memoranda/.

[16] Ibid. FICAM Enterprise Architecture information is available at https://arch.idmanagement.gov/.

[17] Refer to OMB Circular A-11 for more information on strategic planning and strategic reviews: https://www.whitehouse.gov/omb/information-for-agencies/circulars/.

4. Each agency shall incorporate Digital Identity Risk Management[18] into existing Federal processes as outlined in NIST SP 800-63, including the selection of assurance levels commensurate with the risk to their digital service offerings.[19]

    - Agencies shall use these levels to make risk-informed decisions when selecting and using processes and technologies implemented across the ICAM environment.

    - Agencies shall update legacy e-Authentication risk assessments to shift away from the obsolete LOA model.

    - Agencies shall coordinate with state, local, and tribal governments, other entities, and individuals to provide identity verification and access control appropriate to the risk level and performance of the business function in cases where information sharing or collection is required for business and mission functions.

    - Agencies shall share feedback on their implementation of the Digital Identity Risk Management process with the Federal CIO Council, Federal Privacy Council, and NIST to drive improvements to NIST SP 800-63.

Architecture

1. Agencies shall establish authoritative solutions for their ICAM services[20] by rationalizing the ICAM capabilities that they will keep, replace, retire, or consolidate. Agencies are encouraged to promote flexible and scalable solutions that can work across the agency and change as mission needs evolve.

2. Agencies shall ensure that deployed ICAM capabilities are interchangeable, use commercially available products, and leverage open Application Programming Interfaces (APIs) and commercial standards to enable componentized development and promote interoperability across all levels of government.

3. Agencies shall manage the digital identity lifecycle of devices, non-person entities (NPEs), and automated technologies such as Robotic Process Automation (RPA) tools and Artificial Intelligence (AI), ensuring the digital identity is distinguishable, auditable, and consistently managed across the agency. This includes establishing mechanisms to bind, update, revoke, and destroy credentials for the device or automated technology.

---

[18] Requirements in NIST SP 800-63 provide specific guidance related to digital identity risk (inclusive of privacy) that agency relying parties apply while executing all relevant RMF lifecycle phases. Digital identity risk management does not establish additional risk management processes for agencies.

[19] Federal employees and contractors are required to be identity proofed and credentialed in accordance with OMB and OPM policy. Therefore, digital identity risk assessments described in NIST SP 800-63 complement, rather than supersede, the guidance and requirements of HSPD-12.

[20] Information on ICAM services is available at https://arch.idmanagement.gov/services/.

4. Agencies that are authoritative sources for attributes (e.g., SSN) utilized in identity proofing events, as selected by OMB and permissible by law, shall establish privacy-enhanced data validation APIs for public and private sector identity proofing services to consume, providing a mechanism to improve the assurance of digital identity verification transactions based on consumer consent.

    - These selected agencies, in coordination with OMB, shall establish standard processes and terms of use for public and private sector identity proofing services that want to consume the APIs.

5. Agencies shall leverage federated solutions to accept identity and authentication assertions made by mission and business partners.

    - Agencies shall accept assertions by partners based on digital identity risk and associated assurance levels in accordance with NIST guidelines and Government-wide ICAM requirements.[21]

    - Agencies shall confirm that these assertions use open commercially available standards to the extent available.

Acquisition

1. Agencies shall require all contracts requiring contractors to have access to Federally controlled facilities or access to Federally controlled information systems to include a requirement to comply with HSPD-12 and FIPS 201 for affected contractor personnel based on OPM requirements and the Federal Acquisition Regulation (FAR).[22]

2. Agencies shall confirm that products and services acquired to further their HSPD-12 and ICAM implementations are compliant with OMB policy, NIST standards, and supporting technical specifications.[23]

3. Agencies shall leverage approved Best in Class and Tier 2 contract vehicles,[24] or Federally provided shared services, to procure digital certificates for identification and authentication of Federal enterprise identities.

---

[21] This list of requirements for accepting externally issued credentials is available at https://www.idmanagement.gov/.

[22] The Federal Acquisition Regulation, FAR, 48 C.F.R. Subpart 4.13, requires agencies to comply with FIPS 201 for contractors who require routine logical or physical access and includes language to this effect in applicable solicitations and contracts.

[23] Approved products and services, such as those on the GSA Approved Products List (APL) are available at https://www.idmanagement.gov/.

[24] M-19-13 outlines guidance on the implementation of category management principles and use of common contract solutions. For more information, refer to https://www.whitehouse.gov/omb/information-for-agencies/memoranda/.

4. Agencies shall leverage the CDM Program to accelerate their procurement and deployment of tools related to the ICAM capabilities in Phase 2 or future phases.

    - Agencies shall work with the CDM Program to understand requirements and identify future CDM phase capabilities that support ICAM goals.

V. Improving Digital Interactions with the American Public

Improving the trust and safety of transactions with the public across the Federal Government is critical to digital service delivery. It is imperative that agencies manage the risk to services and public user data at a level commensurate with the risk inherent to the digital offering as well as with the sensitivity of the data collected to provide the digital offering.

1. Agencies shall ensure that identity proofing for Federal digital services provided to public consumers aligns with NIST guidance and Government-wide ICAM requirements.

2. Agencies shall limit the collection of PII for establishing an individual's identity to that which is legally authorized, relevant, and deemed reasonably necessary.

    - Once collected, agencies shall ensure that PII is protected commensurate with the level of risk it harbors, which may include the implementation of robust practices and technologies.

3. Agencies shall establish processes based on digital identity risk and associated assurance levels to allow an individual to bind, update, use, and disassociate non-Government-furnished authenticators to their digital identity when accessing Federal digital services provided to public consumers.

4. Agencies shall leverage existing credentials and identity federations that meet the agency's determined acceptable risk level rather than standing up processes or capabilities to issue new credentials to users.

5. Agencies shall use Federally provided or commercially provided shared services,[25] to the extent available, to deliver identity assurance and authentication services to the public.

    - These shared services shall align with NIST SP 800-63 security and privacy requirements.

    - With appropriate consent and privacy protections, agencies should share proofing confirmations across agencies to reduce public burden for having to submit identity data more than once to access Federal Government services.

[25] Information on consumer-facing identity services and solutions are available at https://www.idmanagement.gov/.

- Where appropriate, and when individuals' consent is not obtainable, agencies should modify existing Privacy Act system of record notices to include routine uses permitting the disclosure of proofing information to reduce public burden for having to submit identity data more than once to access Federal Government services.

- Agencies should solicit and document direct feedback from consumers to determine whether there is demand for the use of other service providers. If consumers demand a certain service provider and the provider meets the mission requirements, agencies should consider federating with that credential provider.

- Agencies should use shared service providers that leverage more than one solution to enhance enterprise resiliency in case of a compromise or other service failure.

VI. Enumerating Government-wide Responsibilities

The following agencies lead Government-wide efforts to improve the management and use of digital identity.

The Department of Commerce (DOC) is responsible for the following actions:

1. Publish and maintain, within six months of the issuance of this policy, a roadmap with timelines and milestones for developing new and updating existing NIST guidance related to ICAM;

2. Develop and issue guidance to promote the deployment of technology, including open source software that address agency digital identity needs such as new implementations of technology intended to meet agency use cases for devices, automated technologies, mobile, and cloud;

3. Develop guidance to facilitate deployment and use of derived credentials for logical and physical access using authenticators that satisfy the security and privacy requirements of NIST SP 800-63 while leveraging the PIV identity proofing process;

4. Establish, develop, and maintain resources for federation protocols, identity proofing, and authentication in alignment with NIST SP 800-63;

5. Utilize feedback provided by agencies to make improvements to NIST SP 800-63-3 and other guidance; and

6. Develop criteria, in coordination with the General Services Administration (GSA), for accrediting products and services that meet the assurance levels outlined in NIST SP 800-63.

GSA[26] is responsible for the following actions:

1. Develop and maintain, within six months of the issuance of this policy, a roadmap for providing or updating GSA solutions and shared services that allow agencies to achieve the outcomes in OMB ICAM policy and NIST standards and guidelines;

2. Publish and maintain, within three months of the issuance of this policy, a consolidated catalog of existing ICAM solutions and shared services that agencies can leverage immediately to begin meeting the requirements of this memorandum;

3. Maintain and support, in coordination with OMB and DHS, the evolution of the Government-wide FICAM Architecture and associated guidance, previously published in the *FICAM Roadmap and Implementation Guidance, v2.0: FICAM Playbooks*, and establish and maintain a repository for agency best practices;

4. Maintain and innovate the FIPS 201 evaluation process, and associated Approved Products List (APL), to enable the acquisition of interoperable solutions for physical and logical access control;

5. Determine the feasibility, in coordination with OMB, of establishing or leveraging a public or private sector capability for accrediting ICAM products and services available on GSA acquisition vehicles, and confirm the capability leverages NIST developed criteria for 800-63 assurance levels. This capability should support and not duplicate existing Federal approval processes;

6. Innovate capabilities and update Federal Public Key Infrastructure (PKI)[27] to provide government with a trust framework and infrastructure to administer digital certificates and other authentication solutions, such as those based on public key cryptography. This includes updating the PKI shared service provider approach to enable strong government oversight of service providers, including procurement and cost controls through GSA acquisition solutions as applicable;[28] and

7. Ensure that all GSA acquisition solutions for ICAM meet all relevant law, OMB circulars and policies, Federal Acquisition Regulations, and NIST standards.[29]

---

[26] GSA serves as the executive agency for Government-wide acquisitions of information technology related to identity management initiatives. This designation is given to GSA in accordance with section 5112(e) of the Clinger-Cohen Act of 1996 (40 U.S.C. § 11302(e)). In this capacity, GSA maintains the GSA APL, developed to organize and define a standardized approval process for PIV products and services.

[27] Federal PKI provides the government with a common approach to administer digital certificates and public-private key pairs for specific use cases.

[28] A comprehensive list of certified PKI service providers for the Federal government is available at https://www.idmanagement.gov/.

[29] As part of its agency reform initiatives generally, and Multiple Award Schedule (MAS) Reform initiative specifically, GSA shall strive to implement policies within eighteen (18) months of the effective date of this

OPM is responsible for the following actions:

1. Develop, in coordination with OMB and NIST, a vetting and credentialing model to assist agencies in making an HSPD-12 risk determination for employees, contractors, and other users accessing Federal information systems[30] and information from non-Federally controlled facilities, such as a seasonal employee or an administrator for a cloud service; and

2. Update, within one (1) year of the issuance of this policy, vetting requirements for eligibility for a HSPD-12 aligned credential that enables physical and logical access to Federally controlled facilities and information systems. This update will consolidate applicability requirements from Executive Orders on Suitability and OMB Memo M-05-24, to include applicability specifications for non-U.S. national and temporary agency employees.[31]

DHS is responsible for the following actions:

1. Ensure that the *Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*, and other pertinent Interagency Security Committee (ISC) guidance, are aligned with Government-wide policy for the implementation of PIV credentials;

2. Lead research and development (R&D) coordination with the interagency, private sector, and international partner stakeholders to identify ICAM mission needs with related technology capability gaps, including in particular those that cannot be solved with currently fielded technologies, and that may require additional R&D investment to reach operational deployment maturity; and

3. Develop and publish, in consultation with GSA, OPM, OMB, and DOC a Physical Access Control System (PACS) security and privacy control overlay[32] to help agencies identify core controls for PACS.

---

memorandum which reduce customer confusion, and enhance MAS's internal coordination with respect to HSPD-12 and Physical Access Control Systems (PACS).

[30] Per OMB Circular A-130, "Federal information system" means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency.

[31] *Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12*, https://www.opm.gov/investigations/suitability-executive-agent/policy/.

[32] An "overlay" is a specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. For additional information on developing security control baselines, refer to OMB Circular A-130, *Managing Information as a Strategic Resource*, and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations.* These documents are available at https://www.whitehouse.gov/omb/information-for-agencies/circulars/ and https://csrc.nist.gov/publications.

Rescissions

OMB rescinds the following with the release of this memorandum:

1. M-04-04, *E-Authentication Guidance for Federal Agencies*

2. M-05-05, *Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services*

3. M-06-18, *Acquisition of Products and Services for Implementation of HSPD-12*

4. M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*

5. OMB Memorandum, *Requirements for Accepting Externally-Issued Identity Credentials*, October 6, 2011

Policy Assistance

Address all questions or inquiries regarding this memorandum to the OMB Office of the Federal Chief Information Officer (OFCIO) via email: ofcio@omb.eop.gov.