CIRA SMART CARD ALLIANCE ACCESS CONTROL COUNCIL POSITION PAPER

Smart Card Alliance Commentary: OMB Circular A-130 – Managing Information as a Strategic Resource

Publication Date: September 2016
Publication Number: ACC-16001

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information, please visit http://www.smartcardalliance.org.

Table of Contents

1 Introduction

Circular A-130, "Managing Information as a Strategic Resource," published by the Office of Management and Budget (OMB), sets policy and establishes guidance for management of Federal information resources. As OMB is within the Executive Office of the President, OMB A-130 is authoritative and clarifies policies for both Federal agencies and service providers.

The previous version of Circular A-130 was published in 2000 on the heels of the dot-com collapse, yet before the creation of the Department of Homeland Security (DHS). Much has changed. The world and government have become heavily dependent on information technology (IT) and the security of the IT ecosystem. After the Office of Personnel Management (OPM) data breach and subsequent "cybersecurity sprint," OMB released a new revision of Circular A-130 in July of 2016. The 2016 revision addresses new statutory requirements (e.g., FISMA 2014) and the enhanced technological capabilities that are now available.

The 85-page July 27, 2016 revision[1] can be considered a major rewrite with significant changes throughout the document. The following aspects of the revision are particularly significant to entities involved with logical and physical access control, smart card technology, identity management, and associated security systems:

- Federal Information is now seen as a strategic resource, with a focus on IT, security, data governance, and privacy. Accordingly, the guidance establishes general policy for IT planning, budgeting and funding through governance, acquisition, and management of Federal information, personnel, equipment, IT resources, and supporting infrastructure and services. The guidance includes:
    - Moving from periodic checklist compliance to ongoing monitoring assessment and evaluation, and providing guidance to embrace new technology and solutions
    - Conducting proactive risk management with repeated testing of agency solutions
    - Assigning responsibility and accountability to everyone (government and citizens) for assuring privacy (especially personally identifiable information (PII)) and the security of information
- The guidance establishes the chief information officer (CIO) as THE accountable party and mandates a Senior Agency Official for Privacy (SAOP).
- The guidance reinforces aspects of Homeland Security Presidential Directive 12 (HSPD-12), Federal Information Processing Standard (FIPS) 201, and associated documents, and encapsulates the principles into one authoritative policy document.
- The guidance more explicitly brings the existence of a physical access control system (PACS) under the jurisdiction of the CIO and IT departments, who now clearly have the budgeting, planning, funding, and decision-making authority.

This position paper was developed by the Smart Card Alliance Access Control Council to highlight the impact of the OMB Circular A-130 2016 update on the access control industry, and on government agencies procuring and implementing access control systems. The position paper focuses on highlighting relevant changes in the 2016 update to A-130, discussing the impact of these changes on the Federal government and commercial industry, and outlining issues to be considered in complying with A-130 for selected topic areas.

[1] https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

The position paper summarizes A-130 content (in Section 2) and then extracts key points and provides industry commentary on those points (in Section 3).

2 Summary of OMB Circular A-130 2016

The changes in A-130 2016 generally align with the new and updated information management-related policies, procedures, methodologies, standards, technologies and legislation that have been established over the past 15 years.[2] In addition, A-130 was reorganized to highlight the specific policy areas listed in the introduction. The noteworthy changes that the Smart Card Alliance Access Control Council feels are relevant consist of policies, concepts and approaches for:

- Planning, budgeting and funding
- Security and privacy
- Shared roles and responsibility
- Proactive risk management and real-time knowledge of the environment (continuous monitoring)
- Identity assurance, authentication and public key infrastructure (PKI)

The following content summarizes key content from A-130 in each of these areas.

2.1 Planning, Budgeting and Funding

A-130 2016 augments planning and budgeting policies introduced in A-130 2000, and organizes them into policies related to strategic planning; enterprise architecture; programming and budgeting; and business continuity planning. A-130 also aggregates these disciplines with OMB Circulars A-11, Capital Programming Guide and A-131, Value Engineering.

- OMB Circular A-11, Capital Programming Guide – Defines polices for submitting the federal budget that include agency guidance for capital planning and investment control.
- OMB Circular A-131, Value Engineering – Defines policies for well-established commercial practice for cutting waste and inefficiency that can help Federal agencies reduce program and acquisition costs, improve the quality and timeliness of performance, and take greater advantage of innovation to meet 21st century expectations and demands.

2.2 Security and Privacy

A-130 emphasizes security and privacy as equally important considerations throughout the document. This duality and its significance are best described by the following two quotes from A-130:

1. "While security and privacy are independent and separate disciplines, they are closely related, and it is essential for agencies to take a coordinated approach to identifying and managing security and privacy risks and complying with applicable requirements."
2. "To be effective, information security and privacy considerations must be part of the day-to-day operations of agencies. This can best be accomplished by planning for the requisite security and privacy capabilities as an integral part of the agency strategic planning and risk management processes, not as a separate activity."

Privacy now has the same level of focus as security, which includes OMB's establishment of the Federal Privacy Council. This emphasis on both security and privacy is underscored in A-130 by:

1. Its definition of the Senior Agency Information Security Officer and Senior Agency Official for Privacy roles and responsibilities; and

[2] See OMB's announcement of the release of A-130 2016 for A-130's focus on three key elements to help spur innovation throughout the government, https://www.whitehouse.gov/blog/2016/07/26/managing-federal-information-strategic-resource

2. Its introduction of the information security continuous monitoring and privacy continuous monitoring processes.

In addition, A-130 2016 details responsibilities for designated roles in Appendix I, Responsibilities for Protecting and Managing Federal Information Resources, which covers security responsibilities; and Appendix II, Responsibilities for Managing Personally Identifiable Information, which covers privacy responsibilities.

2.3 Shared Roles and Responsibilities

While A-130 2000 only identified roles and responsibilities for agency chief financial officers (CFOs) and chief information officers (CIOs), A-130 2016 has expanded planning, budgeting, security, privacy and record management roles. The roles are based on the evolution of agency governance, budgeting, human capital, and risk management activities, and responsibilities that have been generally accepted and established since A-130 2000. Roles described in A-130 2016 include:

- Authorizing Official
- Chief Acquisition Officer
- Chief Human Capital Officer
- Chief Information Officer
- Chief Financial Officer
- Senior Agency Information Security Officer
- Senior Agency Official for Privacy
- Senior Agency Official for Records Management

2.4 Proactive Risk Management and Real-Time Knowledge of the Environment[3]

The OMB Circular A-130 2016 emphasizes migrating security checks from static, point-in-time authorization processes to a more dynamic, near-real-time ongoing process. Such continuous and dynamic monitoring has a two-fold intent: 1) maintaining IT system security control operational authorization (i.e., authority to operate (ATO)) via continuous security and privacy monitoring, assessment and system penetration tests; and 2) keeping abreast of and mitigating evolving cybersecurity threats and system vulnerabilities through the use of automated and manual processes. A-130 identifies Information Security Continuous Monitoring (ISCM) and Privacy Continuous Monitoring (PCM) as the methodologies to support the two-fold continuous dynamic monitoring approach.

Real-time knowledge of the environment entails the following: “In order to keep pace, we must move away from periodic, compliance-driven assessment exercises and, instead, continuously assess our systems and build-in security and privacy with every update and re-design. Throughout the Circular, we make clear the shift away from check-list exercises and toward the ongoing monitoring, assessment, and evaluation of Federal information resources.” NIST SP 800-137, “Information Security Continuous Monitoring for Federal Information Systems and Organizations,” September 2011, and “Supplemental Guidance on Ongoing Authorization - Transitioning to Near Real-Time Risk Management,” June 2014, have been identified as the methodology guidance for implementing continuous dynamic monitoring.

Proactive risk management “…emphasizes the need for strong data governance that encourages agencies to proactively identify risks, determine practical and implementable solutions to address said risks, and implement and continually test the solutions. This repeated testing of agency solutions will help to proactively identify additional risks, starting the process anew.”

[3] https://www.whitehouse.gov/blog/2016/07/26/managing-federal-information-strategic-resource

2.5 Identity Assurance, Authentication, and Use of PKI

A-130 sets policy to "deploy effective security controls to provide Federal employees and contractors with multifactor authentication, digital signature, and encryption capabilities that provide assurance of identity and are interoperable Government-wide and accepted across all Executive Branch agencies." This policy area is specific to the use of Personal Identity Verification (PIV) credentials for authentication, encryption, and digital signatures and implementation of the identity proofing guidelines in FIPS 201 and agency-specific background investigations.

3 Smart Card Alliance Commentary on OMB Circular A-130 2016

The Smart Card Alliance Access Control Council reviewed the full OMB Circular A-130, "Managing Information as a Strategic Resource." This section includes specific references in Circular A-130 and the possible industry impact as identified by the commentary contributors.

The tables below include the key points, text and page number from the OMB Circular A-130 and Smart Card Alliance comments on the points for the main body of the document (Section 3.1), Appendix I (Section 3.2) and Appendix II (Section 3.3).

Please note that the text below provides a high level summary of key points in A-130. It is highly recommended that OMB Circular A-130 2016[4] be reviewed in-depth for additional information and details.

3.1 Commentary on OMB Circular A-130 – Main Body of the Document

OMB Circular A-130 Text	Smart Card Alliance Commentary
Policy, page 4: "Agencies shall establish a comprehensive approach to improve the acquisition and management of their information resources by: performing information resources management activities in an efficient, effective, economical, secure, and privacy-enhancing manner; focusing information resources planning to support their missions; implementing an IT investment management process that links to and supports budget formulation and execution; and rethinking and restructuring the way work is performed before investing in new information systems."	This reference emphasizes the importance of IT investment full lifecycle planning, implementation, and evaluation. It is supported by OMB Circulars A-11, Capital Programming Guide, and A-131, Value Engineering. Acquired systems shall be considered based on how they will improve the overall organization mission and goals while enhancing efficiencies and maintaining privacy.
Planning and Budgeting, page 4: "Agencies shall establish agency-wide planning and budgeting processes in accordance with OMB guidance."	FICAM falls under an agency-wide policy that addresses upgrades, or replacements of legacy non-compliant IT systems and components. A -130 prioritizes funding for such IT upgrades.
Strategic Planning Information Management, page 5: "Agencies shall continually facilitate adoption of new and emerging technologies."	Emphasis is to leverage emerging technologies that improve efficiencies and security, and are privacy-enhancing. New technology that supports "continuous monitoring" is also required in order to comply with NIST SP 800-37.

[4] https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

OMB Circular A-130 Text	Smart Card Alliance Commentary
Risk Management, page 6: "Agencies shall consider information security, privacy, records management, public transparency, and supply chain security issues for all resource planning and management activities throughout the system development life cycle so that risks are appropriately managed."	Incorporation of security and privacy considerations shall be included in all phases of resource planning and management, and system development and operations. Security and privacy are equally important throughout the planning and budgeting lifecycle. Continuous monitoring of potential threats for any new system being acquired is mandatory. Monitoring shall not interfere with public transparency.
Enterprise Architecture, page 6: "Agencies shall develop an enterprise architecture (EA) that describes the baseline architecture, target architecture, and a transition plan to get to the target architecture. The agency's EA shall align to their IRM Strategic Plan."	This follows the general principles of the "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance" document.[5] FICAM is therefore the suggested reference that embodies the intent of this policy and its effect on the access control community. Within enterprise architecture practices, an as-is state (baseline architecture) is defined through surveys and reviews of existing systems and components; a target architecture is then defined followed by a gap analysis and migration strategy that allows the agency to migrate from the as-is state to the target state. In conjunction with this effort, there should be a continuous review from a risk management perspective so that the final end state complies with the organization's risk management plan. Both logical and physical access control systems are part of the IT infrastructure and elements of a target architecture.
Planning, Programming, and Budgeting, page 7: "Agencies shall plan, program and budget in accordance with the Federal Information Technology Acquisition Reform Act (FITARA) and related OMB policy."	FITARA outlines specific requirements related to: 1. Agency Chief Information Officer (CIO) authority enhancements 2. Enhanced transparency and improved risk management in IT investments 3. Portfolio review 4. Federal data center consolidation initiative 5. Expansion of training and use of IT cadres 6. Maximizing the benefit of the Federal strategic sourcing initiative 7. Government wide software purchasing program

[5] https://www.idmanagement.gov/IDM/servlet/fileField?entityId=ka0t0000000TNNBAA4&field=File__Body__s

OMB Circular A-130 Text	Smart Card Alliance Commentary
Governance, page 8: "In support of agency missions and business needs, and in coordination with program managers, agencies shall: 1. Define, implement, and maintain processes, standards, and policies applied to all information resources at the agency, in accordance with OMB guidance; 2. Require that the CIO, in coordination with appropriate governance boards, defines processes and policies in sufficient detail to address information resources appropriately; 3. Ensure that the CIO is a member of governance boards that inform decisions regarding IT resources to provide for early matching of appropriate information resources with program objectives. The CIO may designate, in consultation with other senior agency officials, other agency officials to act as their representative to fulfill aspects of this responsibility so long as the CIO retains accountability."	This guidance assigns responsibility and accountability to appropriate officials. In addition, Section 5b - Governance; Section 5c - Leadership and Workforce; Appendix I, page 19, and Appendix II, page 2, cover how agencies shall assign responsibilities and accountability to specific titles within each agency to achieve compliance with requirements in OMB Circular A-130. This is the first A-130 document that included specific language for accountability. Emphasis is on comprehensive oversight of all information systems and their uniform compliance to OMB guidance which now include NIST Special Publications and other FICAM related documents. Systems covered include credentialing systems and physical access control systems.
Leadership and Workforce, page 10: "Agencies shall require that the Chief Human Capital Officer (CHCO), CIO, CAO, and SAOP develop a set of competency requirements for information resources staff, including program managers, information security, privacy, and IT leadership positions."	Personnel now need to meet competency requirements in order to work and manage and lead activities or programs. Certifications demonstrating specific competencies are available from a number of organizations including: the Smart Card Alliance (CSCIP/G and CSEIP); Cisco (CCNA-Security and SCYBER); Computing Technology Industry Association (CASP); International Council of E-Commerce Consultants (CEH); International Information Systems Security Certifications Consortium (CISSP, CAP, ISSAP, ISSEP, ISSMP and SSCP); Information Systems Audit and Control Association (CISM and CISA); the SANS Institute Global Information Assurance Certifications (GCIA, GCED, GCFA, GCIH, GSEC, GSLC and GSNA); and the Program Management Institute (PMP). Each certification program is tailored to specific disciplines and has its own requirements for obtaining and maintaining the certification. Please consult the sponsoring organization's web site for current information.

OMB Circular A-130 Text	Smart Card Alliance Commentary
IT Investment Management, page 10, Acquisition of Information Technology and Services: "Agencies shall make use of adequate competition, analyze risks (including supply chain risks) associated with potential contractors and the products and services they provide, and allocate risk responsibility between Government and contractor when acquiring IT;"	Past performance and subject matter credibility will go a long way to building a trust relationship between a government agency and a contractor. This statement acknowledges the complexity and risks of IT investments and provides guidance that considers best value in the acquisition of information technology and services.
Agency Approval, page 11: "Agencies shall ensure that all acquisition strategies, plans, and requirements (as described in FAR Part 7), or interagency agreements (such as those used to support purchases through another agency) that include IT are reviewed and approved by the purchasing agency's CIO."	Accountability is given to the CIO to assure acquisition strategies have approval at the highest level.
Investment Planning and Control, page 12: "Agencies are responsible for establishing a decision-making process that shall cover the life of each information system and include explicit criteria for analyzing the projected and actual costs, benefits, and risks, including information security and privacy risks, associated with the IT investments. Agencies shall designate IT investments according to relevant statutes, regulations, and guidance in OMB Circular A-11, and execute processes commensurate with the size, scope, duration, and delivery risk of the investment. The IT investment processes shall encompass planning, budgeting, procurement, management, and assessment. For further guidance related to investment planning, refer to OMB Circular A-11, including the Capital Programming Guide**."**	IT investment lifecycle management is a requirement along with defined criteria to establish total cost of ownership and to assure projected and actual costs are tracked. IT investments need to be specifically made that address size, scope, and duration. OMB Circular A-11, Capital Programming Guide, is the key reference for this policy.
Selection Criteria and Requirements, page 13: "Agencies shall consider the following factors when analyzing IT investments: Qualitative and quantitative research methods are used to determine the goals, needs, and behaviors of current and prospective managers and users of the service to strengthen the understanding of requirements."	In developing requirements for IT investments, agencies shall use qualitative and quantitative research methods to better understand the goals and needs of managers and users to assure that the IT requirements will fulfill these goals and objectives.
IT Investment Design and Management, page 13: "Agencies shall implement the following requirements: Information systems and processes must support interoperability and access to information; IT investments must facilitate interoperability, application portability, and	IT investments must support interoperability, portability and scalability on heterogeneous platforms such that standards can facilitate disparate access to information. Interoperability supports multiple access from different platforms but also increases the importance and need for

OMB Circular A-130 Text	Smart Card Alliance Commentary
scalability across networks of heterogeneous hardware, software, and communications platforms; Information systems, technologies, and processes shall facilitate accessibility under the Rehabilitation Act of 1973, as amended; in particular, see specific electronic and IT accessibility requirements commonly known as "section 508" requirements (29 U.S.C. § 794d);"	security and access management.

3.2 Commentary on OMB Circular A-130, Appendix I - Responsibilities for Protecting and Managing Federal Information Resources

The requirements in Appendix I represent those areas deemed to be of fundamental importance to achieving effective agency information security programs and those areas deemed to require specific emphasis by OMB.

OMB Circular A-130 Text: Appendix I	Smart Card Alliance Commentary
Page 4: "Agencies shall plan and budget to upgrade, replace, or retire any information systems for which security and privacy protections commensurate with risk cannot be effectively implemented."	Funding is prioritized for upgrade or replacement of non-compliant systems.
Page 6: "Agencies shall adhere to Government-wide requirements in the deployment and use of identity credentials used by employees and contractors accessing Federal facilities."	The A-130 statement and GSA Inspector General (IG) reports[6] explicitly state that PACS shall adhere with NIST SP 800-116, "A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)." See also the GSA IG reports on the use of non-compliant ID cards. No non-compliant PACS or identity credentials shall be used. Refer to the GSA Approved Products List (APL) on IDManagement.gov[7] for approved products and service providers, and to NIST SP800-116[8] for deployment guidance. NIST SP 800-116 provides additional information on the use of PIV credentials, the Government-wide standard identity credential, in

[6] https://www.gsaig.gov/sites/default/files/ipa-reports/OIG%20EVALUATION%20REPORT_Facility%20Specific%20Building%20Badges.pdf
https://www.gsaig.gov/sites/default/files/ipa-reports/OIG%20EVALUATION%20REPORT_GSA%20Management%20of%20Contractor%20HSPD-12%20PIV%20Cards.pdf

[7] https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000Sfwo

[8] http://csrc.nist.gov/publications/drafts/800-116r1/sp800_116_r1_draft.pdf

OMB Circular A-130 Text: Appendix I	Smart Card Alliance Commentary
	physical access control systems. Physical access controls systems, which include servers, databases, workstations and network appliances in either shared or isolated networks, are considered information systems.
Page 9: "Agencies should generally categorize information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII at the moderate or high confidentiality impact level."	PACS are included in this category.
Page 12: "Agencies shall prohibit the use of unsupported information systems and system components, and ensure that systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement."	This guidance prioritizes funding for replacing or upgrading legacy systems in the budget planning.
Page 13: "Agencies shall: 11) Require use of multifactor authentication for employees and contractors in accordance with Government-wide identity management standards." [Footnote 94] [Footnote 94] "Pursuant to Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, NIST FIPS 201 describes the initial Government-wide identity management standard for employees and contractors as a smartcard form factor (the PIV card). With the emergence of a newer generation of computing devices and in particular with mobile devices, the use of PIV cards has evolved technically to include other form factors that can be deployed directly with mobile devices as specified in NIST SP 800-157. The PIV credential associated with this alternative is called a Derived PIV Credential. Derived PIV Credentials are based on the general concept of derived credentials in NIST SP 800-63. Issuing a Derived PIV credential to PIV card holders does not require repeating identity proofing and vetting processes. The user simply proves possession and control of a valid PIV Card to receive a Derived PIV Credential."	This allows a PIV high assurance identity credential of alternative form factors to the PIV card to be embedded in a mobile device. The mobile device can then be used with multifactor authentication to log-on to agency IT resources.
Page 15, Footnote 101: "Agencies have flexibility in implementing the baseline controls in SP 800-53; however, agencies are required to justify, in their security plans or overlays, any tailoring actions."	Agencies must have justification in their security plan if it deviates from SP 800-53.

OMB Circular A-130 Text: Appendix I	Smart Card Alliance Commentary
Page 19: "Authorizing officials have budgetary oversight for an information system or be responsible for the mission or business operations supported by the system. Through the authorization process, authorizing officials are responsible and accountable for the risks associated with information system operations. Because information security is closely related to the privacy protections required for PII, authorizing officials are also responsible and accountable for the privacy risks that arise from the operation of an information system."	This guidance assigns responsibility and accountability to authorizing officials. In addition, Section 5b - Governance; Section 5c - Leadership and Workforce; Appendix I, page 19, and Appendix II, page 2, cover how agencies shall assign responsibilities and accountability to specific titles within each agency to achieve compliance with requirements as mandated in OMB Circular A-130. This is the first A-130 document which includes specific language for accountability. Also see comment on Governance, page 8 in Section 3.1.
Page 19: "Agencies must ensure that periodic testing and evaluation of the effectiveness of information security and privacy policies, procedures, and practices are performed with a frequency depending on risk, but at least annually."	This guidance means that the protective measures are to be maintained and remain current.
Page 24, Digital Signatures: "Digital signatures can mitigate a variety of security vulnerabilities by providing authentication and non-repudiation capabilities, and ensuring the integrity of Federal information whether such information is used in day-to-day operations or archived for future use. Additionally, digital signatures can help agencies streamline mission or business processes and transition manual processes to more automated processes to include, for example, online transactions. Because of the advantages provided by this technology, OMB expects agencies to implement digital signature capabilities in accordance with Federal PKI policy, and NIST standards and guidelines. For employees and contractors, agencies must require the use of the digital signature capability of Personal Identity Verification (PIV) credentials. For individuals that fall outside the scope of PIV applicability, agencies should leverage approved Federal PKI credentials when using digital signatures."	The update requires that agencies shall: • Deploy effective security controls to provide Federal employees and contractors with multifactor authentication, digital signature, and encryption capabilities that provide assurance of identity and are interoperable Government-wide and accepted across all Executive Branch agencies. • Develop and implement processes to support use of digital signatures, a form of electronic signature, for employees and contractors. Digital signatures were not required for compliance with earlier PIV card readers. This guidance is an upgrade that may require reader replacements. (See GSA APL on IDManagement.gov web site for a listing of compliant readers.) (See also digital signature requirements in OMB A-130: page 19 – g. 3); Appendix I-6 – c. 10); Appendix I-13, i. 12); Appendix I-24 – n).)
Page 24, Identity Assurance: "Identity assurance is an essential element of an effective information security program. To streamline the process of citizens, businesses, and other partners securely accessing Government services online requires a risk-appropriate demand of identity assurance. Identity assurance, in an online context, is the ability	Government agencies need to identify new identity assurance methods outside of the scope of PIV and PIV-I credential issuance for access to Federal information resources by citizens, businesses, and other partners.

OMB Circular A-130 Text: Appendix I	Smart Card Alliance Commentary
of an agency to determine that a claim to a particular identity made by an individual can be trusted to actually be the individual's true identity. Citizens, businesses, and other partners that interact with the Federal Government need to have and be able to present electronic identity credentials to identify and authenticate themselves remotely and securely when accessing Federal information resources. An agency needs to be able to know, to a degree of certainty commensurate with the risk determination, that the presented electronic identity credential truly represents the individual presenting the credential before a transaction is authorized. To transform processes for citizens, businesses, and other partners accessing Federal services online, OMB expects agencies to use a standards-based federated identity management approach that enables security, privacy, ease-of-use, and interoperability among electronic authentication systems."	

3.3 Commentary on OMB Circular A-130, Appendix II: Responsibilities for Managing Personally Identifiable Information

OMB Circular A-130 Text: Appendix II	Smart Card Alliance Commentary
Page 3: "Agencies are required to designate a Senior Agency Official for Privacy (SAOP) who has agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risks."	This is the first A-130 document that includes specific language for roles, responsibilities and accountability. This guidance assigns responsibility and accountability to appropriate officials. In addition, Section 5b - Governance; Section 5c - Leadership and Workforce; Appendix I, page 19, and Appendix II, page 2, cover how agencies shall assign responsibilities and accountability to specific titles within each agency to achieve compliance with requirements in OMB Circular A-130.
Page 5: "Agencies shall designate a Senior Agency Official for Privacy. The head of each agency shall designate an SAOP who has agency-wide responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program to ensure compliance with	See above comment Page 3.

OMB Circular A-130 Text: Appendix II	Smart Card Alliance Commentary
all applicable statues, regulations, and policies.”	
Page 6: Agencies shall provide performance metrics and reports.	See above comment Page 3.

4 Conclusions

The 2016 update to the OMB Circular A-130, "Managing Information as a Strategic Resource," is an important milestone for the Federal government in its initiatives to improve the security of government information systems. The document provides an overarching framework of guidance that incorporates many of the Federal initiatives of the past 15 years.

For Federal agencies implementing and industry suppliers providing logical and physical access control, smart card technology, identity management, and associated security systems, the guidance:

- Provides a continued strong focus on the need for implementing updated Federal information systems that address information security and privacy.
- Reinforces the requirements of HSPD-12 and FIPS 201 and the use of the PIV credential for Federal employees and contractors.
- Defines PACS as an information system that is under the jurisdiction of the CIO and IT departments.
- Assigns responsibility to specific agency staff for modernization of IT resources.
- Requires agencies to prioritize funding for modernization of IT resources.

The Smart Card Alliance believes that OMB Circular A-130 will help Federal agencies implement identity and information security systems more efficiently and effectively.

5 Publication Acknowledgements

This position paper was developed by the Smart Card Alliance Access Control Council to highlight the impact of the OMB Circular A-130, Managing Information as a Strategic Resource 2016 update, on the access control industry and on government agencies procuring and implementing access control systems.

Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Access Control Council members for their contributions. Participants involved in the development of this position paper included: Defense Manpower Data Center (DMDC); General Services Administration (GSA); ID Technology Partners; IQ Devices; Parsons/Secure Missions Solutions; SigNet Technologies, Inc.; XTec, Incorporated.

The Smart Card Alliance thanks the following Council members who wrote content and participated in the development of this document:

- **Tim Baldridge**, DMDC
- **Mark Dale**, XTec, Inc.
- **Tony Damalas**, SigNet Technologies
- **Dave Helbock**, XTec, Inc.
- **Daryl Hendricks**, GSA
- **Mike Kelley**, Parsons/Secure Missions Solutions
- **Cathy Medich**, Smart Card Alliance
- **Steve Rogers**, IQ Devices
- **Mike Strock**, Smart Card Alliance
- **Lars Suneborn**, Smart Card Alliance
- **Rob Zivney**, ID Technology Partners

Trademark Notice

About the Smart Card Alliance Access Control Council

The Smart Card Alliance Access Control Council is focused on accelerating the widespread acceptance, use, and application of smart card technology for physical and logical access control. The group brings together, in an open forum, leading users and technologists from both the public and private sectors and works on activities that are important to the access control community and that will help expand smart card technology adoption in this important market. The Council works on projects to stimulate the use of smart card technology for access control.