Office of Management and Budget Circular A-130 "Managing Information as a Strategic Resource"

Carol Bales

Federal Computer Security Managers' Forum

August 17, 2016

Circular A-130:
Managing Information as a Strategic Resource

- Circular A-130 serves as the overarching policy and framework for Federal Information Resources Management
- First update in 16 years was released July 28, 2016
- Significant revisions made to reflect current statute, Executive Orders, Presidential Directives, government-wide policies, standards, and practices

Applicability

- Applies to:
  - The information resources management activities of all agencies of the Executive Branch of the Federal Government.
  - Management activities concerning all information resources in any medium (unless otherwise noted), including paper and electronic information.
- Does not apply to national security systems, but are encouraged to do so where appropriate.

Significance of A-130 to Federal Cybersecurity

- Addresses the three main structural challenges to sustained progress for the Cybersecurity National Action Plan released earlier this year. Those challenges include:
  - Cyber workforce vacancies;
  - Legacy IT; and
  - Fragmented governance of IT across the federal landscape.

Overview: Main Body

Focuses on planning and budgeting, governance, workforce development, IT investment management, privacy and information security, leveraging the evolving Internet, records management, and information management and access.

In support, agencies are required to:

- Develop and maintain an IRM Strategic Plan
- Ensure the terms and conditions of contracts and other agreements are:
  - linked to the IRM strategic plan goals; and
  - sufficient to enable agencies to meet their policy and legal requirements

Overview: Appendix I

- Provides the Responsibilities for Protecting Federal Information Resources, including:
  - The minimum requirements for Federal information security programs;
  - Federal agency responsibilities for the security of information and information systems; and
  - The requirements for Federal privacy programs, including specific responsibilities for privacy program management.
- Acknowledges that the concepts of information security and privacy are inexorably linked
- Requires the application of risk management, information security, and privacy policies beginning with the IT acquisition process
- Places ultimate and full responsibility with agency heads

Overview: Appendix II

- Addresses the management of Personally Identifiable Information (PII)
- The reporting and publication requirements of the Privacy Act of 1974 have been revised and reconstituted as OMB Circular A-108
- Establishes the requirement for a Senior Agency Official for Privacy (SAOP) at each agency
- Establishes a set of fair information practice principles (FIPPs)
- Also requires agencies to:
  - Determine if information systems contain PII
  - Consider the sensitivity of PII and determine which privacy requirements may apply and any other necessary safeguards
  - Conduct Privacy Impact Assessments (PIAs) as required by the E-Government Act of 2002
  - Reduce their holdings of PII to the minimum necessary level for the proper performance of authorized agency functions

Risk Management

Agencies are required to:

- Regularly review and address risk regarding processes, people, and technology
- Implement a risk management framework
- Address risk throughout the system development life cycle
- Implement supply chain risk management principles

Workforce Planning

Agencies are required to:

- Develop a set of competency requirements for information resources staff, and develop and maintain a workforce planning process
- Ensure the workforce has appropriate knowledge and skills
- Implement innovative approaches and track performance of workforce development training
- Take advantage of flexible hiring authorities for specialized positions
- Ensure the SAOP is involved in the hiring, training, and professional development needs of the agency with respect to privacy

Inventories and Legacy IT

Agencies are required to:

- Maintain an inventory of major information systems
  - Includes contractor information systems operated on behalf of agencies
- Maintain an inventory of PII
- Upgrade, replace or retire systems that cannot be appropriately protected or secured
  - Includes phasing out unsupported system components

Note: All information systems are subject to the requirements of the FISMA whether or not they are designated as a major information system.

Strong Authentication, Digital Signature and Encryption

- Require use of multifactor authentication for employees and contractors
- Encrypt all FIPS 199 moderate-impact and high-impact information at rest and in transit, unless encrypting such information is technically infeasible
- Develop and implement processes to support use of digital signatures for employees and contractors

Continuous Monitoring and Ongoing Authorization

- Reaffirms the requirements of M-14-03 and NIST 800-37 to implement an information security continuous monitoring program
- Agencies are required to:
  - Transition information systems and common controls to an ongoing authorization process
  - Address recommendations of the SAOP as part of the system authorization process
  - Implement use of leveraged and joint authorizations, as appropriate

Specific Safeguarding Measures

- In addition to addressing and tailoring controls in NIST SP 800-53, agencies are required to implement specific safeguarding measures, such as:
  - Implementing a policy of least functionality, least privilege, and separation of duties
  - Isolating sensitive or critical information resources into separate security domains
  - Implementing access control policies for information resources and using two-factor authentication
  - Protecting administrator, user, and system documentation
  - Continuously monitoring, logging, and auditing the execution of information system functions by privileged users
  - Implementing and maintaining current updates and patches

Cybersecurity Framework

- NIST is responsible for maintaining a Cybersecurity Framework to reduce cyber risks to critical infrastructure.
- Agencies can leverage the Cybersecurity Framework to complement their current information security programs.
- NIST is responsible for providing guidance on how agencies can use the Cybersecurity Framework and in particular, how the Risk Management Framework and Cybersecurity Framework, can work together.

Contract Requirements

Agencies are required to:

- Ensure that terms and conditions in contracts and other agreements are sufficient to meet security requirements
  - Includes ensuring that terms and conditions of contracts and other agreements include sufficient provisions for Federal Government notification and access
- Provide oversight of information systems used or operated by contractors or other entities
- Ensure that requirements of the Privacy Act apply to a Privacy Act system of records when a contractor operates the system of records on behalf of the agency

Incident Detection, Response and Recovery

Agencies are required to:

- Develop and implement incident management policies, and maintain formal incident response capabilities and mechanisms
- Designate sensitive positions and execute commensurate security clearance levels for appropriate agency personnel
- Establish clear roles and responsibilities
- Periodically test incident response procedures
- Document lessons learned for incident response and update procedures
- Ensure that processes are in place to verify corrective actions
- Report incidents to OMB, DHS, the CIO, the SAOP, inspectors general and general counsel, law enforcement, and Congress in accordance with procedures issued by OMB

Next Steps

- Agencies to implement the requirements of A-130, and notify OMB where additional clarification is needed
- NIST to update guidelines, as needed, to ensure consistency with A-130
- OMB to update “M” memos, as needed
- OMB to continue to measure agencies’ progress on implementing the requirements in A-130


EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
OFFICE OF MANAGEMENT AND BUDGET


OMB
CYBER

POC

- Carol_A._Bales@omb.eop.gov