Seizing the opportunity

Protecting information from cyber attacks through OMB Circular A-130

KPMG Government Institute

Issue brief | November 2016

On July 28, 2016, the Office of Management and Budget (OMB) issued the first update to Circular A-130 since 2000.[1] This Circular applies to all federal agencies, including their services providers.[2] The revised Circular recognizes the dramatic changes in the information and information technology (IT) landscape and the rapid pace of change. The revised Circular recognizes the opportunities to strengthen the business of government through digital delivery of program and services. Previously titled *Management of Federal Information Resources,* the revised Circular is titled *Managing Information as a Strategic Resource*, signaling a shift in expectations. The revised Circular also recognizes the critical importance of managing "information systems in a way that addresses and mitigates security and privacy risks associated with new information technologies and new information processing capabilities."

This issue brief focuses on the information security and privacy aspects of Circular A-130. Having worked extensively with governments and private sector companies in the United States and globally on these issues, we offer perspectives on what we view as critical elements of an information protection strategy.

The priority focus on cybersecurity

Technology risks go far beyond securing e-mail servers, business systems, social media, mobile and digital devices, and cloud-based services. Today, government has to be concerned about securing the Internet of Things, smart grids, software robotics, intelligent systems, and wearables, with additional innovative technology right around the corner. IT risk management is about responsibly balancing risk and reward in adopting emerging technology and protecting valued information assets and personally identifiable information (PII) on citizens and organizations.

Federal information systems are potentially highly vulnerable to hackers. The Office of Personnel Management (OPM) data breach, resulting in the loss of personnel and personal information of 22 million Americans, demonstrates what can go wrong. Cybersecurity concerns have been on the Government Accountability Office's (GAO) high-risk list since 1997.[3]

The stakes only continue to increase with the massive proliferation of new information, adoption of emerging technology, antiquated legacy IT systems, stovepiped accountability structures, and the ever-expanding capabilities to penetrate systems. Cyber attacks are widely recognized as one of our top national security threats.

As discussed in a report on the results of a survey of executive-level government officials and contractors by (ISC)[2] and KPMG LLP titled *The State of Cybersecurity from the Federal Cyber Executive Perspective*, "The reality that cyber attacks once considered preventable are now regarded as inevitable has long been understood and acknowledged by cyber professionals, but this reality is just now reaching the masses due to media coverage of high-profile breaches in recent years. The increased public scrutiny has added to the federal government's enormous task of defending itself against an infinite number of attackers."

[1] OMB Circular A-130, *Managing Information as a Strategic Resource,* July 28, 2016 (https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf).

[2] National security systems are covered by other requirements.

[3] GAO "HIGH-RISK SERIES: An Update, GAO-15-290, February 2015 (http://gao.gov/assets/670/668415.pdf). See high-risk area "Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information."

From the security director of a civilian federal agency: "The playing field is tilted in favor of the adversary. To alter this reality, a fundamental shift is required in how the government approaches cybersecurity."[4]

Among key survey findings:

- 59 percent of respondents say that their agency struggles to understand how cyber attackers could potentially breach their systems.
- 65 percent of respondents disagree that the federal government as a whole can detect ongoing cyber attacks.
- The lack of accountability was consistently identified as a top challenge, with some respondents unable to identify a senior leader in their agency whose sole responsibility is cybersecurity.
- People can be their organization's greatest cybersecurity asset or greatest liability, with 42 percent of respondents indicating that people are currently their greatest vulnerability to cyber attacks.

Circular A-130 cybersecurity requirements in a nutshell

Circular A-130 establishes ***general policy*** regarding management of information security and privacy risk. Appendices I and II provide ***additional detail*** regarding agency responsibilities for protecting and managing federal information resources and PII.

Appendix I, *Responsibilities for Protecting and Managing Federal Information Resources*, establishes requirements for information security and privacy programs and provides guidance on a coordinated approach to information security management. Included are requirements for federal agencies to:

- Implement an *agency-wide risk management process* for the ongoing management of information security and privacy risk across three levels: (1) organization, (2) business or process, and (3) information systems
- Develop, implement, document, maintain, and oversee *agency-wide information security and privacy programs*, encompassing people, processes, and technologies. Included are requirements for:
  - Agency information security and privacy policies, planning, budgeting, management, implementation, and oversight
  - Protection of information and systems from unauthorized access, use, disclosure disruption, modification, and/or destruction by providing for confidentiality, integrity, and availability
  - Adequate security over all information the federal government creates, collects, processes, stores, transmits, and disposes of, including government information in contractor systems and networks
  - A risk management framework to support (1) information and systems categorization; (2) selection, implementation, and assessment of security controls; (3) authorization and reauthorization of information systems[5] and common IT controls; and (4) continuous information system control monitoring
  - Adoption of systems security engineering principles, concepts, and techniques to facilitate development, deployment, operation, and sustainment of trustworthy and adequately secured systems over the IT system life cycle
  - Timely awareness by the chief information officer (CIO) and the senior agency official for privacy (SAOP) of any system or information component that cannot be appropriately protected or secured and are high-priority for upgrade, replacement, or system retirement. In addition, where corrective actions are longer term, agencies are to take interim remediation measures until such time as full remediation actions are completed.
- Require agencies with which they share PII to maintain the information in a system that has a *confidentiality impact level*[6] consistent with the impact level established by the agency sharing the information
- Impose *conditions* (including specified security and privacy controls), in written agreements with agencies with which they share PII, governing creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of the shared information.

[4] *The State of Cybersecurity from the Federal Cyber Executive Perspective*, (ISC)² and KPMG LLP, May 19, 2016 (http://www.kpmg-institutes.com/content/dam/kpmg/governmentinstitute/pdf/2016/federal-cyber-survey.pdf).

[5] Authorization process decisions are established under OMB Circular A-130, in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4 and SP 800-137. Circular A-130 includes the concept of ongoing authorization, which entails a continuous process of reevaluation.

[6] Confidentiality impact levels are established under the NIST Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.

Appendix II, *Responsibilities for Managing Personally Identifiable Information*, addresses responsibilities for managing PII. This Appendix outlines general responsibilities, summarizes key privacy requirements in other sections of Circular A-130, and provides implementation guidance for protecting PPI. Agencies are required to:

- Apply the *Fair Information Practice Principles* (FIPPs), which are a collection of widely accepted principles used to evaluate information systems, processes, programs, and activities affecting individual privacy
- Designate an SAOP
- Develop, document, implement, and maintain a *comprehensive agency-wide privacy program*, including people, processes, and technologies
- Manage PII collected for statistical purposes under a *pledge of confidentiality*.

Critical elements of an information protection strategy

As agencies begin to implement the Circular A-130 information protection requirements, they can look to the Circular and its appendices for guidance. They also must consider the ever-changing dynamic of cybersecurity, which for the foreseeable future will be impacted by emerging innovative technologies and evolving insider and outsider threats. In the United States and globally, KPMG has observed leading cybersecurity practices and offers for consideration elements of a practical cybersecurity implementation strategy. These elements are intended to work together and represent transformational change in the way federal agencies, their personnel, and contractors address growing information security and privacy risks.

1. **Establish senior-level commitment** to managing IT and privacy risk and **cascade that commitment down the chain of command**, so everyone (not just the cyber workforce) understands their responsibility.
2. **Identify and plan for resources** to implement and maintain an information system and privacy program throughout the life cycle of each information system. As discussed in *The State of Cybersecurity from the Federal Cyber Executive Perspective*, there is a need to place more focus on the human element and implement a more balanced approach as it relates to the people + process + technology equation. More technology alone will not protect information systems from cyber attack. It is critical to build and retain highly skilled cyber talent. Leading organizations adopt agency-wide cyber-education programs that go beyond basic awareness.
3. **Identify and rank current and emerging cyber risks** based on management's determination of the potential risk impact and likelihood of occurrence.
4. **Assess existing information security and privacy controls** and other actions to mitigate identified risks, which could encompass reducing, accepting, avoiding, and/or sharing the risk when a gap is identified. This process includes (a) collaboration across all levels and organizations within the agency and with contractors and other stakeholders and (b) assessments that test controls to ensure they are properly designed and operating effectively as expected, such as table-top exercises to simulate cyber attacks.
5. **Establish and implement an Information Security Continuous Monitoring (ISCM) program and a Privacy Continuous Monitoring (PCM) program**, premised on an understanding of the agency's cyber risk tolerance and used day-to-day to manage security and privacy risk throughout the agency.
6. **Use the results of the ISCM program to support the CIO's authorization and reauthorization decisions** for information systems under Circular A-130.
7. **Establish a process for the SAOP to review and approve the privacy impact** of information system prior to authorization and reauthorization under Circular A-130.
8. **Establish and implement a comprehensive security and privacy incident reporting and remediation program** to provide a mechanism for continual enhancement.
9. **Establish and implement an inclusive contingency planning program** to provide for the recovery and reconstitution of information systems to a known and secure state after a disruption, compromise, or failure.
10. **Monitor and enforce the Circular A-130 requirement for contractors and third parties** to adhere to the agency's established security and privacy program policies to manage the risk to the agency. Also, require agencies with which the agency shares PII to maintain the information in a system that has a confidentiality impact level consistent with the impact level established by the agency for its PII.

How KPMG can help

KPMG LLP (KPMG) is a leader in helping federal agencies and other governmental organizations in the United States and globally identify and assess information security and privacy risks and develop associated actions and controls to mitigate risk to an acceptable level. KPMG has extensive experience applying the NIST Risk Management Framework.[7] This enables us to offer applicable experience working with information systems and applying a thorough framework and monitoring the risk throughout the life cycle of the system.

KPMG brings the "know-how" to critical elements by working with leaderships across the federal government to design, implement, and/or evaluate the effectiveness of security and privacy programs. Our services include, but are not limited to, assistance with the following:

- Evaluating agency-level and system-level risk management programs, including the impact to information security and privacy
- Evaluating existing information security and privacy continuous monitoring programs
- Recommending, designing, and/or implementing mitigation actions to support the effort of reducing cyber risk to the agency.

[7] The Risk Management Framework (RMF) is established under NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*.

Contact us

Tony Hubbard
Principal, Federal Advisory – Cyber Lead
T: 703-286-8320
E: thubbard@kpmg.com

Geoff Weber
Principal, Federal Advisory
T: 703-286-8480
E: glweber@kpmg.com

Jason Gould
Director, Federal Advisory
T: 703-286-6896
E: jagould@kpmg.com

The KPMG Government Institute was established to serve as a strategic resource for government at all levels, and also for higher education and not-for-profit entities seeking to achieve high standards for accountability, transparency, and performance. The Institute is a forum for ideas, a place to share leading practices, and a source of thought leadership to help governments address difficult challenges such as performance management, regulatory compliance, and fully leveraging technology.

Visit www.kpmg.com/us/governmentinstitute.

Jeffrey C. Steinhoff
Managing Director, KPMG Government Institute
T: 703-286-8710
E: jsteinhoff@kpmg.com

kpmg.com/socialmedia