

December 4, 2015

White House Office of Management and Budget
725 17th Street, N.W.
Washington, D.C. 20503

Re: Public comment on proposed revisions to Circular No. A-130, *Managing Information as a Strategic Resource*

Dear White House Office of Management and Budget:

Thank you for the opportunity to comment on the proposed revisions to Circular No. A-130, *Managing Information as a Strategic Resource*.

With more than 100,000 members, ACM (Association for Computing Machinery) is the world's largest educational and scientific computing society, uniting computing educators, researchers, and professionals to inspire dialogue, share resources, and address the field's challenges. These comments were developed by the ACM U.S. Public Policy Council (USACM), which serves as the focal point for ACM's interaction with the U.S. government in all matters of U.S. public policy related to information technology. ACM U.S. Public Policy Council statements represent the views of the Council and do not necessarily represent the views of the Association.

Privacy and Security

We commend OMB on striving to treat privacy in a manner consistent with how security is treated in the draft Circular No. A-130. However, we believe this goal has not been fully achieved in the current version. Although the document is appropriately even-handed in many places, such as when it calls in the policy section for equivalent strategies and plans for privacy and security, there are many other places where security is mentioned in isolation. In some cases, this is justified by differences between security and privacy. However, where guidance is as relevant for privacy as for security, we recommend that the Circular explicitly address both.

Where privacy is invoked in addition to security, the relative emphasis should be comparable. The current emphasis differs noticeably. One particularly important example of this involves the integration of security and privacy into engineering processes. Although the importance of this is stated for both privacy and security, security receives much greater and more specific attention on this issue, which is unfortunate given the steadily increasing prominence of the Privacy by Design movement¹ and the pursuit of "privacy engineering" by, among others, the National Institute of Standards and Technology (NIST).² The criticality of effectively inserting privacy, beyond performing privacy impact assessments (PIAs), into system acquisition and development life cycles warrants greater substance, and we strongly encourage OMB to expand its treatment of privacy in this regard.

The Circular should include explicit language describing the importance and expectation of coordination between security and privacy functions at all levels. The virtues of cross-functional security coordination at multiple organizational levels are well known, and these efforts have often included privacy. More recently, moves toward enterprise risk management have created larger and more flexible spaces for systematic cross-functional coordination aimed at ensuring an appropriate risk posture.³ It is surprising, therefore, that the value of such coordination goes largely unmentioned in the current draft.

Open Source Software

All development types of software, including open source software, should be considered to meet agency needs, and the Circular should make this clear. Open source software can constitute an important option for government agencies. Proprietary, internally developed, and open source software each have their own advantages and disadvantages. The U.S. Department of Defense CIO issued guidance in the 2009 memorandum, "Clarifying Guidance Regarding Open Source Software (OSS)," which states that, in almost all cases, open source software meets the definition of "commercial computer software."⁴ Further, the guidance found that the Department's information assurance rules do not forbid the use and adoption of open source software by the government and its contractors.

Thank you again for the opportunity to comment on the proposed revisions to Circular No. A-130 and for your efforts to update this important policy document for federal agencies. The staff and members of the ACM U.S. Public Policy Council are available if you have questions or would like additional information about the issues raised in this public comment.

Sincerely,



Eugene H. Spafford, Ph.D.
Chair, U.S. Public Policy Council (USACM)
Association for Computing Machinery



Christopher Bronk, Ph.D.
Chair, Digital Governance Committee
U.S. Public Policy Council (USACM)

¹ Stuart S. Shapiro. 2010. Privacy By Design: Moving From Art to Practice. Commun. ACM 53, 6 (June 2010), 27-29, DOI=<http://dx.doi.org/10.1145/1743546.1743559>.

² National Institute of Standards and Technology (NIST), Privacy Engineering, http://csrc.nist.gov/projects/privacy_engineering/.

³ NIST Special Pub. 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, Appendix D, 2011, <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>.

⁴ U.S. Department of Defense, CIO, Memorandum, Clarifying Guidance Regarding Open Source Software (OSS), Oct. 16, 2009, <http://dodcio.defense.gov/Portals/0/Documents/OSSFAQ/2009OSS.pdf>.