UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

NOV 18 2014

MEMORANDUM FOR: Chief Information Officers, Privacy Officers, and Information Technology Security Officers

FROM: Catrina D. Purvis
Chief Privacy Officer (CPO)

Frederick Stephens
Deputy Assistant Secretary for Administration

Steven I. Cooper
Chief Information Officer (CIO)

SUBJECT: Commerce Policy Regarding 1) Implementing National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Appendix J Privacy Controls, and 2) Senior Agency Official for Privacy (SAOP) Approval as a Precondition for the Issuance of an Authorization to Operate (ATO)

Public trust and confidence in the privacy practices of federal agencies is essential to government operations and individual privacy. This memorandum establishes Commerce policy to implement the privacy provisions of Office of Management and Budget (OMB) Memorandum 14-04, and provides implementation guidance.

- Commerce Bureaus and Operating Units (OUs) are expected to implement the privacy controls in Appendix J to satisfy the privacy requirements set forth in the 1974 Privacy Act and any privacy-related policies published by OMB.

- The Commerce SAOP/ CPO shall identify which of the common Appendix J privacy controls shall be provided by the Department. The Bureau/Operating Unit Chief Privacy Officer (BCPO) shall ensure that the remainder of Appendix J privacy controls will be allocated as common, system, or hybrid, consistent with the Bureau and/or OU's mission/ business needs and risk tolerance.

- An assessment of compliance with applicable Appendix J privacy controls must be conducted by the BCPO, who shall serve as the Commerce SAOP/CPO's designated representative for this activity.

- A Commerce SAOP/CPO signed Privacy Impact Assessment (PIA) shall be required prior to the following: 1) issuance of an ATO for any new system which will collect,

process, share, and/or store personally identifiable information (PII)[1] and 2) re-issuance/ renewal of an ATO to authorize changes on a legacy PII processing, sharing, and/or storage system, which will create new privacy risks[2], including adding a new collection of PII. This will ensure that the new and/or modified collection, processing, sharing, and/or storage of PII has been determined to be legally authorized, compliant, and necessary by the SAOP/CPO who serves as the Department's information steward for PII and Privacy Act covered records.

- BCPO signature shall also be required on all PIAs, as well as Privacy Threshold Analyses (PTAs). The BCPO signature authority for PIAs and PTAs may be delegated only to the CIO and/or Deputy CIO. Accordingly, the Commerce PIA and PTA templates have been revised and are effectively immediately.

- Please ensure appropriate attention to and priority of these activities within your bureau. Questions regarding this memorandum should be directed to the Commerce CPO, Dr. Catrina D. Purvis at 202-482-3463 and CPurvis@doc.gov.

cc: Mike Maraya, Acting Chief Information Security Officer

Attachments

Privacy Threshold Analysis Template
Privacy Impact Assessment Template

[1] Information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, biometric records, etc., alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. [OMB M-07-16].
[2] New privacy risks include, but are not limited to, conversions, anonymous to non-anonymous, significant system management changes, significant merging, new public access, commercial sources, new interagency uses, internal flow or collection, and alteration in character of data.