CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2025.03.27 17:31:41 -04'00'

Approved for Release Date
Charles R. Cutshall
Chief Privacy Officer and Director of Open Government

DEPARTMENT OF COMMERCE
OFFICE OF PRIVACY AND OPEN GOVERNMENT

PRIVACY BULLETIN #2025-001 (FY2025)

SUBJECT: Privacy Threshold Assessment and Privacy Impact Assessment Exemption for Information Technology that collects, maintains, or disseminates Federal Employee and Contractor System Administration and Audit Data.

EFFECTIVE DATE: Upon release of this Privacy Bulletin.

EXPIRATION DATE: Effective until superseded or revoked.

SUPERSEDES: Not applicable.

PURPOSE: This Bulletin exempts the Office of the Secretary and the Department of Commerce's (Department) operating units[1] from the requirement to conduct a privacy threshold assessment (PTA) and privacy impact assessment (PIA) when the only information in an identifiable form[2] that is collected, maintained, or disseminated using information technology[3] is system administration and audit data (SAAD) that pertains to federal employees and contractors.

[1] The operating units of the U.S. Department of Commerce are organizational entities outside the Office of the Secretary charged with carrying out specified substantive functions (i.e., programs) of the Department. *See* Department Organizational Order (DOO) 1-1, *Mission and Organization of the Department of Commerce*.

[2] *See* the E-Government Act of 2002 (Public Law 10-347) (E-Government Act) at § 208(b)(1). As defined in the E-Government Act, 'identifiable form' means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. *Id.* at § 208(d).

[3] 'Information technology' means

(A) with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—
  (i) of that equipment; or
  (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(B) includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but

(C) does not include any equipment acquired by a federal contractor incidental to a federal contract.

SCOPE: This bulletin applies to all information technology that is authorized to operate by the Office of the Secretary and the Department's operating units.[4]

This bulletin pertains to SAAD, which includes information such as User ID, Internet Protocol (IP) address, and date and time of access, and which is information in an identifiable form because it is information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.[5]

If the SAAD pertains to members of the general public, such as information technology that hosts public-facing interfaces (e.g., websites), a PTA and/or PIA is still required. In addition, a PTA and/or PIA is still required for information technology that is used to monitor for threats or vulnerabilities (e.g., a security information and event management (SIEM) system).

BACKGROUND: The privacy provisions of the E-Government Act of 2002 (E-Government Act) require federal agencies to conduct a PIA before developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form. OMB's guidance implementing the privacy provisions of the E-Government Act clarifies that no PIA is required where information relates to internal government operations, as in the following circumstances:

1. For government-run websites, IT systems, or collections of information, to the extent that they do not collect or maintain information in identifiable form about members of the general public; and,
2. If agencies are developing IT systems or collecting non-identifiable information for a discrete purpose, not involving matching with or retrieval from other databases that generate information in identifiable form.[6]

The Department's *Guide to Effective Privacy Impact Assessments (PIA)*[7] provides a framework for conducting PIAs and a methodology for assessing how personally identifiable information (PII)[8] is to be managed in electronic information systems. It requires that a PIA be conducted

---

See 40 U.S.C. § 11101(6).

[4] In some instances, an information system may receive an 'Authorization to Use' in lieu of an 'Authorization to Operate' (e.g., FedRAMP authorized information systems and shared services). An 'Authorization to Use' is a type of 'Authorization to Operate' and is covered by this bulletin.

[5] All information in an identifiable form is PII, but not all PII is information in an identifiable form. The definition of PII is necessarily broad and includes information that is not in an identifiable form, but that can be used to distinguish or trace an individual's identity when it is combined with other information that is linked or linkable to a specific individual.

[6] *See* OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (September 26, 2003).

[7] Available at https://www.commerce.gov/sites/default/files/opog/PIA_Guide_September_2020.pdf.

[8] 'Personally identifiable information' means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (*See* OMB Circular A-130)

when developing or procuring any new information technology or system that collects or processes PII, including SAAD.

CONTROLS: This bulletin supplements the Department's implementing guidance for National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (updated Dec. 2020), RA-8 Privacy Impact Assessments.

Operating unit privacy officials are responsible for selecting and implementing privacy controls for information systems that process PII and should work with system owners during Requirements Definition (RMF Task P-15) to define the privacy requirements for the information system, which includes determining whether a PIA is required.[9]

PROCEDURE: The responsibilities of key stakeholders are as follows:

1. Operating unit privacy officials shall:[10]

- Review the information system[11] documentation to understand what information[12] is being processed (or will be processed) by the information system.
- Determine whether the information system's information resources[13] process (or will process) SAAD and whether the SAAD pertains to only federal employees and contractors.[14]

[9] *See* U.S. Department of Commerce's Security and Privacy Assessment & Authorization (SPA&A) Handbook.
[10] Consistent with OMB Memorandum M-16-24, the Department's Chief Privacy Officer and Director of Open Government (who serves as the Department's Senior Agency Official for Privacy (SAOP)) may delegate certain privacy functions assigned to the SAOP to the Office of the Secretary Privacy Officer and operating unit privacy officials. Those officials may within the context of their respective operating unit have the title 'Privacy Officer' or 'Bureau Chief Privacy Officer,' or the functions may have been delegated to an official with another title such as 'Chief Information Officer' or 'Chief Administrative Officer.' The Office of the Secretary Privacy Officer serves as the privacy official for the Office of the Secretary and is responsible for all privacy-related functions similarly delegated to or assigned to operating unit privacy officials. In all cases, however, the Chief Privacy Officer and Director of Open Government retains responsibility and accountability for the Office of the Secretary's and operating units' privacy programs, which includes any privacy functions performed by operating unit privacy officials.
[11] 'Information system' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (*See* 44 U.S.C. § 3502(8))
[12] 'Information' means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. (*See* OMB Circular A-130)
[13] 'Information resources' means information and related resources, such as personnel, equipment, funds, and information technology. (*See* 44 U.S.C. § 3502(6))
[14] At the discretion of the operating unit's privacy official, a privacy threshold assessment (PTA) may be conducted and used to document whether the information system's information resources process (or will process) SAAD and whether the SAAD pertains to only federal employees and contractors. Although a PTA may be submitted to the Chief Privacy Officer and Director of Open Government in lieu of the Exemption Memorandum (Appendix A), this office's preference is for the operating unit's privacy official to submit the Exemption Memorandum.

- If the SAAD only pertains to federal employees and contractors, complete the Exemption Memorandum (Appendix A) and submit it to the Office of Privacy and Open Government at CPO@doc.gov.
- If the Exemption Memorandum is approved by the Chief Privacy Officer and Director of Open Government, ensure that the Exemption Memorandum is included in the information system's authorization package[15] as an artifact supporting the decision to not select and implement the control (RA-8 Privacy Impact Assessments).[16]

2. Chief Privacy Officer and Director of Open Government shall:

- Review the Exemption Memorandum.
- Determine whether to approve or deny the request within ten (10) working days.
- Return the determination to the operating unit's privacy official.

PROGRAM CONTACT INFORMATION:

Office of Privacy and Open Government
(202) 482-1190
CPO@doc.gov

[15] 'Authorization package' means the essential information that an authorizing official uses to determine whether to authorize the operation of an information system or the use of a designated set of common controls. At a minimum, the authorization package includes the information system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones. (*See* OMB Circular A-130)
[16] Consistent with the Department's Enterprise Cybersecurity Policy, the Cyber Security Assessment and Management (CSAM) application is the Department's formal system of record for all FISMA-reportable information systems inventory and security assessment and authorization management.

APPENDIX A

MEMORANDUM FOR: Charles R. Cutshall
Chief Privacy Officer &
Director of Open Government

FROM: [INSERT NAME]
Operating Unit Privacy Official
[INSERT OPERATING UNIT]

SUBJECT: Operating Unit Privacy Official Request for Privacy Threshold Assessment (PTA) and Privacy Impact Assessment (PIA) Exemption for System Administration and Audit Data.

I have reviewed the information system documentation and/or authorization package for the information system identified below and have determined that the only PII that is being processed (or will be processed) by the information is System Administration and Audit Data (SAAD) that pertains to federal employees and contractors.

Therefore, consistent with Privacy Bulletin ##**2025-001 (FY2025)**, I request that the following information system be exempt from the requirement to conduct a PTA and/or PIA:

Information System: [INSERT NAME].

Information System Description: [INSERT DESCRIPTION].

[DIGITAL SIGNATURE]

[INSERT NAME]
Operating Unit Privacy Official
[INSERT OPERATING UNIT]

I have reviewed the request to exempt the information system identified above from the requirement to conduct a PTA and/or PIA and [APPROVE/DENY] the request.

[DIGITAL SIGNATURE]

Charles R. Cutshall
Chief Privacy Officer &
Director of Open Government