



[Notice-IEB-2024-05; Docket No. 2024-0002; Sequence No. 23]

Privacy Act of 1974; System of Records

AGENCY: General Services Administration (GSA).

ACTION: Notice of a modified system of records.

SUMMARY: GSA proposes to modify a system of records subject to the Privacy Act of 1974, as amended. The system of records was established to collect and maintain records needed by the Office of Inspections to carry out its responsibilities pursuant to the Inspector General Act of 1978, as amended. The Office of Inspector General (OIG) is statutorily directed to provide leadership and coordination and recommend policies for activities relating to programs and operations of the General Services Administration, to promote economy, efficiency, and effectiveness in the administration of such programs and operations, and to prevent and detect fraud, waste, and abuse in such programs and operations. Accordingly, the records in this system are used in the course of inspections and evaluations, and other special projects as determined by the Inspector General. The previously published notice is being revised to add four new routine uses and make changes to update the System Of Records Notice (SORN).

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE **FEDERAL REGISTER**].

ADDRESSES: Comments may be submitted to the Federal eRulemaking Portal, <http://www.regulations.gov>. Submit comments by searching for GSA/ADM-25, Inspection Case Files.

FOR FURTHER INFORMATION CONTACT: Call or email Richard Speidel, Chief Privacy Officer at 202-969-5830 and gsa.privacyact@gsa.gov.

SUPPLEMENTARY INFORMATION: GSA proposes to modify a system of records subject to the Privacy Act of 1974, 5 U.S.C. 552a. GSA intends to add four new routine uses that are consistent with the purposes of this system of records.

GSA proposes adding a routine use (routine use “o”) and revising routine use “p” to reflect the current Office of Management and Budget (OMB) breach response guidance in M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information.

The Inspector General Empowerment Act of 2016 (IGEA), 5 U.S.C. 406(j), exempts certain computerized data comparisons performed by or in coordination with Inspectors General from the Computer Matching and Privacy Protection Act of 1988, Pub. L. 100-503. GSA proposes adding a new routine use (routine use “r”) to clarify that the GSA Office of Inspector General (OIG) has authority to compare OIG records contained in the system with the records of other Federal agencies and non-Federal records.

GSA also proposes adding two additional routine uses. The first is a new routine use (routine use “s”) to permit disclosures to the Office of Personnel Management (OPM), Government Accountability Office (GAO) and the Office of Management and Budget (OMB) in accordance with their responsibilities for evaluating Federal programs. The second is a routine use (routine use “t”) to allow GSA OIG to disclose pertinent records in any legal proceeding before a court or administrative body where GSA or GSA OIG is a party.

Additionally, GSA is making changes to the SORN to update the information in the SORN. In addition to making minor technical and administrative corrections and changes to format, GSA proposes: (1) updating the system location to include secure servers maintained by third-party secure providers to support the procurement of solutions or processes that may require the support of third-party service providers; (2) changing the name of the system of record; (3) providing a new description of the purpose of the

SORN to better summarize the purpose of this system of records; (4) updating the categories of records in the system and the records source categories; (5) adding a section for the categories of individuals covered by the system; (6) updating the location of electronic records, record storage and safeguarding procedures to reflect new technology and procedures used to protect government records; and (7) changing the notification, access, and amendment procedures to align with the corresponding GSA Code of Federal Regulations. The proposed revisions are compatible with the purpose of this system of record.

Richard Speidel,
Chief Privacy Officer,
Office of the Deputy Chief Information Officer,
General Services Administration.

[Billing Code: 6820-AB]

SYSTEM NAME AND NUMBER: Inspection Case Files, GSA/ADM-25

SECURITY CLASSIFICATION: Unclassified

SYSTEM LOCATION: The system is maintained electronically and in paper form at the GSA Office of Inspector General, 1800 F Street, NW, Washington, DC 20405.

Original and duplicate systems may exist, in whole or in part, at secure sites and on secure servers maintained by third-party service providers for the GSA OIG. These systems are FedRAMP Moderate compliant and have all applicable Federal Information Security Modernization Act (FISMA), Federal Information Processing Standards (FIPS), and security controls as applicable.

SYSTEM MANAGER(S): Director, Information Technology of the Office of Inspector General, General Services Administration (JPM), 1800 F Street, NW, Washington, DC 20405.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: General authority to maintain the system is contained in the Inspector General Act of 1978, as amended, 5 U.S.C. 401-424.

PURPOSE(S) OF THE SYSTEM: The OIG maintains this system of records to carry out its responsibilities pursuant to the Inspector General Act of 1978, as amended. The OIG is statutorily directed to provide leadership and coordination and recommend policies for activities relating to programs and operations of the General Services Administration, to promote economy, efficiency, and effectiveness in the administration of such programs and operations, and to prevent and detect fraud, waste, and abuse in such programs and operations. Accordingly, the records in this system are used in the course of inspections and evaluations, and other special projects as determined by the Inspector General.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The system contains records pertaining to present and former GSA and OIG employees, applicants

for employment with GSA and GSA OIG, individuals who have filed a complaint with GSA or GSA OIG, individuals who have provided information to inspections and evaluations, government contractors and employees of government contractors, and individuals referenced in potential or actual cases and matters being examined by the Office of Inspections.

CATEGORIES OF RECORDS IN THE SYSTEM: Inspection files contain information such as name, date, place of birth, contact information, social security number, experience, work-history, and other material that is used in GSA OIG inspections, evaluations, and operations.

RECORD SOURCE CATEGORIES: Records are collected from other systems, individuals and their representatives, present and former GSA and OIG employees, witnesses, complainants, other Federal and State agencies, non-Federal entities, data services, employers, references, co-workers, government contractors, educational institutions, and public sources.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

In addition to other disclosures generally permitted under subsection (b) of the Privacy Act of 1974, 5 U.S.C. 552a(b), the GSA OIG may disclose records for the following routine uses:

- a. A record of any case in which there is an indication of a violation or potential violation of law, whether civil, criminal, or regulatory in nature, may be disseminated to the appropriate Federal, State, local, or foreign agency charged with the responsibility for investigating or prosecuting such a violation or charged with enforcing or implementing the law.
- b. A record may be disclosed to a Federal, State, local, or foreign agency or to an individual or organization in the course of investigating a potential or actual violation of

any law, whether civil, criminal, or regulatory in nature, or during the course of a trial or hearing or the preparing for a trial or hearing for such a violation, if there is reason to believe that such agency, individual, or organization possesses information relating to the investigation, and disclosing the information is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant.

c. A record relating to a case or matter may be disclosed in an appropriate Federal, State, local, or foreign court or grand jury proceeding in accordance with established constitutional, substantive, or procedural law or practice, even when the agency is not a party to the litigation.

d. A record relating to a case or matter may be disclosed to an actual or potential party or to his or her attorney for the purpose of negotiation or discussion on matters such as settlement of the case or matter, plea-bargaining, or informal discovery proceedings.

e. A record relating to a case or matter that has been referred by an agency for investigation, prosecution, or enforcement or that involves a case or matter within the jurisdiction of any agency may be disclosed to the agency to notify it of the status of the case or matter or of any decision or determination that has been made or to make such other inquiries and reports as are necessary during the processing of the case or matter.

f. A record relating to a case or matter may be disclosed to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States, or to an Executive agreement.

g. A record may be disclosed to a Federal, State, local, foreign, or international law enforcement agency to assist in crime prevention and detection or to provide leads for investigation.

h. A record may be disclosed to a Federal, State, local, foreign, Tribal, or other public authority in response to its request in connection with the assignment, hiring or retention of an individual and/or employee, or disciplinary or other administrative action

concerning an employee, the issuance or revocation of a security clearance, the reporting of an investigation of an individual and/or employee, or the award of a contract, grant, or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter.

i. A record may be disclosed to news media and the public in order to provide information related to an inspection or evaluation when the Inspector General determines there exists a legitimate public interest, unless the Inspector General determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

j. A record may be disclosed to an appeal, grievance, hearing, or complaint examiner; an equal opportunity investigator, arbitrator, or mediator; and/or an exclusive representative or other person authorized to investigate or settle a grievance, complaint, or appeal filed by an individual who is the subject of the record.

k. A record may be disclosed as a routine use to a Member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the request of the person who is the subject of the record.

l. Information may be disclosed at any stage of the legislative coordination and clearance process to the Office of Management and Budget (OMB) for reviewing private relief legislation as set forth in OMB Circular No. A-19.

m. A record may be disclosed: (a) to an expert, a consultant, or contractor of GSA or GSA OIG engaged in a duty related to an agency function to the extent necessary to perform the function; and (b) to a physician to conduct a fitness-for-duty examination of a GSA or GSA OIG officer or employee.

n. A record may be disclosed to any official charged with the responsibility to conduct qualitative assessment reviews of internal safeguards and management procedures employed in inspection operations. This disclosure category includes members of the

Council of the Inspectors General on Integrity and Efficiency and officials and administrative staff within their chain of command, as well as authorized officials of the Department of Justice and the Federal Bureau of Investigation.

o. To appropriate agencies, entities, and persons when (1) GSA and/or GSA OIG suspects or has confirmed that there has been a breach of the system of records; (2) GSA and/or GSA OIG has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, GSA and/or GSA OIG (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with GSA's and/or GSA OIG's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

p. To another Federal agency or Federal entity, when GSA and/or GSA OIG determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

q. To the National Archives and Records Administration (NARA) for records management purposes.

r. A record may be disclosed to compare such record with records in other Federal agencies' systems of records or to non-Federal records.

s. To the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), and the Government Accountability Office (GAO) in accordance with their responsibilities for evaluating Federal programs.

t. In any legal proceeding, where pertinent, to which GSA or GSA OIG is a party before a court or administrative body.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Electronic records and backups are stored on secure servers and accessed only by authorized personnel, in accordance with GSA OIG IT Security Policy. Paper files are stored in locked rooms or filing cabinets with access limited to authorized personnel.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: System records are retrievable by searching for information in the case file, including but not limited to, name of an individual, case name, case number, or social security number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF

RECORDS: System records are retained and disposed of according to GSA's records maintenance and disposition schedules and the requirements of the National Archives and Records Administration.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Records in the system are protected from unauthorized access and misuse through a combination of administrative, technical, and physical security measures. Administrative measures include but are not limited to policies that limit system access to individuals within an agency with a legitimate business need, and regular review of security procedures and best practices to enhance security. Technical measures include but are not limited to system design that allows authorized system users access only to data for which they are responsible per FISMA requirements; required use of strong passwords that are frequently changed; and use of encryption for certain data transfers using current FIPS compliant protocols. Physical security measures include but are not limited to the use of data centers which meet government requirements for storage of sensitive data. Paper files are stored in locked rooms or filing cabinets and can only be accessed by authorized users.

RECORD ACCESS PROCEDURES: This system of records is exempt from certain notification, access, and amendment procedures of the Privacy Act, as described below.

However, GSA OIG will consider individual requests to determine whether or not information may be released. If an individual wishes to access any record pertaining to him or her in the system, that individual should consult the GSA's Privacy Act implementation rules available at 41 CFR part 105-64.2.

CONTESTING RECORD PROCEDURES: If an individual wishes to contest the content of any record pertaining to him or her in the system, that individual should consult the GSA's Privacy Act implementation rules available at 41 CFR part 105-64.4.

NOTIFICATION PROCEDURES: Individuals seeking notification of any records about themselves contained in this system of records should contact the system manager at the address above. Follow the procedures on accessing records in 41 CFR part 105-64, subpart 105-64.2 to request such notification.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

a. In accordance with 5 U.S.C. 552a(j), this system of records is exempt from all provisions of the Privacy Act of 1974 with the exception of subsections (b); (c)(1) and (2); (e)(4)(A) through (F); (e)(6), (7), (9), (10), and (11); and (i) of the Act, to the extent that information in the system pertains to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals; to the activities of prosecutors, courts, and correctional, probation, pardon, or parole authorities; and to (a) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (b) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, that is associated with an identifiable individual; or (c) reports of enforcement of the criminal laws, from arrest or indictment through release from supervision. This system is exempted to maintain the efficacy and integrity of the Office of Inspector General's law enforcement function.

In accordance with 5 U.S.C. 552a(k), this system of records is exempt from subsections (c)(3); (d); (e)(1); (e)(4)(G), (H), and (I); and (f) of the Privacy Act of 1974 to the extent that the system consists of investigatory material compiled for law enforcement purposes, other than material within the scope of 5 U.S.C. 552a(j). However, if an individual is denied any right, privilege, or benefit to which the individual would otherwise be eligible as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of the Act, under an implied promise that the identity of the source would be held in confidence; and

b. To the extent the system consists of investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of the Act, under an implied promise that the identity of the source would be held in confidence.

This system has been exempted to maintain the efficacy and integrity of lawful investigations conducted pursuant to the Office of Inspector General's law enforcement responsibilities and responsibilities in the areas of Federal employment, government contracts, and access to security classified information.

HISTORY: This notice revises the previously published notice (73 FR 22383, April 25, 2008).