ode: 6325-47

OFFICE OF PERSONNEL MANAGEMENT

Privacy Act of 1974; System of Records

AGENCY: U.S. Office of Personnel Management, Office of the Chief Information Officer.

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, and the Office of Management and Budget (OMB) Circular No. A-108, notice is given that the Office of Personnel Management (OPM) proposes to establish a new system of records titled, "OPM/Internal-3, Information Technology, Information System, and Network Activity and Access Records." This new system is established to reflect changes in technology, including the increased ability of OPM to link individuals to information technology, information system, or network activity, and to better describe OPM's records linking individuals to reported cybersecurity incidents or their access to certain OPM information technologies, information systems, and networks through the internet or other authorized connections.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is effective upon publication, subject to a 30-day period in which to comment on the routine uses, described below. Please submit any comments by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit written comments by one of the following methods:

- Federal Rulemaking Portal: https://www.regulations.gov. Follow the instructions for submitting comments. All submissions received must include the agency name and docket number for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing at https://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

- The public, Office of Management and Budget (OMB), and Congress are invited to submit any comments by mail to the Office of Personnel Management, ATTN: Senior Agency Official for Privacy, Office of the Director, 1900 E St., NW, Washington, DC 20415, or by email to privacy@opm.gov.

FOR FURTHER INFORMATION CONTACT: OPM Chief Information Officer, Office of Personnel Management, 1900 E Street, NW., Washington, DC 20415, (202) 606-1700 or ocio@opm.gov.

SUPPLEMENTARY INFORMATION: In accordance with the Federal Information Security Modernization Act of 2014, among other authorities, OPM is responsible for complying with information security policies and procedures requiring information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of OPM information and information systems. *See, e.g.*, 44 U.S.C. 3554 (2018). Consistent with these requirements, OPM must ensure that it maintains accurate audit and activity records of the observable occurrences on its information systems and networks (also referred to as ''events'') that are significant and relevant to the security of OPM information and information systems. These audit and activity records may include, but are not limited to, information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. Additionally, monitored events— whether detected utilizing information systems maintaining audit and activity records, reported to the OPM by information system users, or reported to the agency by the cybersecurity research community and members of the general public conducting good faith vulnerability discovery activities—may constitute occurrences that (1) actually or imminently jeopardize, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. OPM has developed a formal

process to track and document these reported ‘‘incidents,’’ which may, in limited circumstances, include records of individuals reporting, or otherwise associated with, an actual or suspected event or incident. This new system of records covers OPM’s tracking of all OPM information technology, information system, and/or network activity, including any access, whether authorized or unauthorized, by users to any OPM information technology, OPM information systems, and/or OPM networks. These records assist OPM’s information security professionals in protecting OPM data, ensuring the secure operation of OPM information systems, and tracking and documenting incidents reported to the agency. The establishment of this new systems notice reflects the need for OPM to monitor users’ connections to OPM’s information systems through the internet or other authorized network connections, as well as to link the identity of individuals or subjects associated with an actual or suspected event or incident for security and administrative purposes. In accordance with Privacy Act requirements of 5 U.S.C. 552a(r), OPM has provided a report to OMB and to Congress on this newly established system of records.

Office of Personnel Management.

Jerson Matias,
Federal Register Liaison.

SYSTEM NAME AND NUMBER: OPM/Internal-3**,** Information Technology, Information System, and Network Activity and Access Records.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Records will be maintained electronically at the Office of Personnel Management offices other sites utilized by OPM, and in information technology, information systems, or networks owned, operated by, or operated on behalf of OPM. Most records will be maintained electronically at one or more of OPM's facilities including, but not limited to: 1900 E St, NW, Washington, DC 20415. Records may also be maintained at the individual information technology or end point of activity within the OPM network, and may be located locally on the physical information technology or end point before being consolidated and stored for analysis and investigation. Records within this system of records may be transferred to an OPM authorized cloud service provider, where records would be limited to locations within the Continental United States. Access to these electronic records includes all locations at which OPM System Managers operate or are supported, including but not limited to the Theodore Roosevelt Building, 1900 E St. NW, Washington, DC 20415. Some or all system information may also be duplicated at other locations where OPM has granted direct access to support OPM System Manager operations, system backup, emergency preparedness, and/or continuity of operations. To determine the location of particular records maintained in this system of records, contact the system manager using the contact information listed in the ''SYSTEM MANAGER(S)'' paragraph, below.

SYSTEM MANAGER(s): OPM Chief Information Officer, ocio@opm.gov, 1900 E St. NW, Washington, DC 20415. Correspondence and/or requests from individuals may be referred to the Chief Information Security Officer and/or Chief Information Officer.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: The Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551 *et seq*.; Executive Order No. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017); OMB

Circular A– 130, Managing Information as a Strategic Resource (2016); OMB Memorandum M–17–12, Preparing for and Responding to a Breach of Personally Identifiable Information (Jan. 3, 2017); OMB Memorandum M–20–32, Improving Vulnerability Identification, Management, and Remediation (Sept. 2, 2020); 5 U.S.C. 301; and 5 U.S.C. 1103.

PURPOSE(S) OF THE SYSTEM: The purpose of this system of records is to ensure that OPM can track information system access and implement information security protections commensurate with the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of OPM information and information systems. Records in this system of records are used by system administrators and security personnel, persons authorized to assist these personnel, and managers for the purpose of: reviewing and analyzing OPM information and OPM information system activity and access events for indications of inappropriate, unusual, or abnormal activity; tracking, documenting, and handling cybersecurity events and incidents; drafting, reviewing, and revising OPM audit and accountability policies; supporting audit reviews, analyses, reporting requirements, and after-the fact investigations of events; planning and managing system services; and otherwise performing their official duties. Authorized OPM personnel may use the records in this system for the purpose of investigating improper access or other improper activity related to information system access; investigating user activity for disciplinary, conduct, or other such action; or, where the record(s) may appear to indicate a violation or potential violation of the law, referring such record(s) to an appropriate law enforcement agency for investigation.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The categories of individuals covered by this system encompass all individuals who are provided OPM information technology, access OPM information systems, or transmit information across the OPM network. This includes: individuals who use authorized OPM information technology, information systems, and/or networks to send or receive OPM information or OPM related communications, access internet sites, or access any OPM information technologies, information

systems, or OPM information; individuals from outside OPM who communicate electronically with OPM users, OPM information technologies, OPM information systems, and/or OPM networks; individuals reporting, tracking, documenting and/or otherwise associated with cybersecurity incident and/or event activities; and any individuals who attempt to access OPM information technologies, OPM information systems, and/or OPM networks, with or without authorization.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system of records may include:

a. Access and activity logs that establish the types of events that occurred on an information system; when the events occurred; where the events occurred; the source of the events; the outcome of the events; and the identity of any individuals or subjects associated with the events. Such information includes, but is not limited to: time stamps recording the data and time of access or activity; source and destination addresses; user, device, and process identifiers, including internet Protocol (IP) address, Media Access Control (MAC) address, and event descriptions; success/fail indications; filenames involved; full text recording of privileged commands; and/or access control or flow control rules invoked. Such information may be collected and aggregated by the operating system or application software locally within an information technology, information system, or network.

b. Information relating to any individuals accessing OPM information, OPM information technologies, OPM information systems, or OPM networks, including but not limited to: Records contained within OPM/Internal-14, Photo Identification and Visitor Access Control Records, 64 FR 73108 (Dec. 29, 1999); user names; persistent identifiers (such as a User ID); contact information, such as title, office, component, and agency; and the authorization of an individual's access to systems, files, or applications, such as signed consent forms or Rules of Behavior forms, or access authentication information (including but not limited to passwords, challenge questions/answers used to confirm/validate a user's identity, and other authentication

factors).

c. Records on the use of electronic mail, instant messaging, other chat services, electronic call detail information (including name, originating/receiving numbers, duration, and date/time of call), and electronic voicemail.

d. Records of internet access from any information technology connected to an OPM information system, on an OPM network, or through authorized connections to OPM networks and OPM information systems, including the IP address of the information technology being used to initiate the internet connection and the information accessed.

e. Audit reviews, analyses, and reporting, including but not limited to, audits that result from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, physical access, and communications at the information system boundaries.

f. Actual or suspected incident or event report information, including but not limited to: Information related to individuals reporting, tracking, documenting and/or otherwise associated with a cybersecurity incident and/or event; information related to reporting, tracking, investigating, and/or addressing an incident or event (*e.g.*, data/time of the incident or event; location of incident or event; type of incident or event; storage medium information; safeguard information; external/internal entity report tracking; data elements associated with the incident or event; information on individuals impacted; information on information system(s) impacted; remediation, response, or notification actions; lessons learned; risk of harm and compliance assessments); and information related to discovering, testing, reporting, tracking, investigating, and/or addressing a security vulnerability or indicator of a security vulnerability.

RECORD SOURCE CATEGORIES: Records covered by this system of records are generated internally (i.e., information technology, information system, and/or network activity logs) regardless of the location from which an individual accesses OPM information or OPM

information systems, manually sourced from OPM personnel, or sourced directly from the individual on whom the record pertains.

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

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system of records may be disclosed outside of OPM as a routine use pursuant to 5 U.S.C. 552a(b)(3) under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purposes for which the information was collected:

a. To any person, organization, or governmental entity in order to notify them of a serious terrorist threat for the purpose of guarding against or responding to such a threat.

b. To Federal, state, local, territorial, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

c. Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the for investigating or prosecuting such violation or charged with enforcing or implementing such law.

d. Pursuant to 5 CFR 295, in an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when OPM determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

e. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, interagency agreement, or other assignment for the Federal government, when necessary to accomplish an agency function related to this system of records.

f. To designated officers and employees of state, local, territorial, or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision.

g. To appropriate officials and employees of a federal agency or entity that requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.

h. To a former employee of OPM for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable agency regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where OPM requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

i. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

j. To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

k. To appropriate agencies, entities, and persons when (1) OPM suspects or has confirmed that there has been a breach of the system of records; (2) OPM has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, OPM (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 OPM's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

l. To another Federal agency or entity, when OPM 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.

m. To such recipients and under such circumstances and procedures as are mandated by federal statute.

n. To the Department of Justice when (a) OPM, or any component thereof; (b) any OPM employee in their official capacity; (c) any OPM employee in their individual capacity where the Department of Justice has agreed to represent the employee; or (d) the United States, where OPM determines that litigation is likely to affect OPM or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by OPM to be relevant and necessary to the litigation.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records in this system of records are stored on paper and/or in electronic form. Records are stored securely in accordance with applicable Executive Orders, statutes, and agency implementing recommendations.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are collected in real time from all OPM information technologies and endpoints on the OPM network and aggregated in databases searchable by identifying characteristics, including, but not limited to, name, user ID, email address, or IP address. Records may be retrieved as part of routine network and information system security monitoring, cybersecurity incident response, database activity monitoring, or in support of other administrative or security investigations in accordance with appropriate laws, rules, and policies.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records of verification, authorization, access, and other activities generated by OPM information technologies, OPM information systems, and/or OPM networks shall be retained in accordance with applicable records schedules, including but not limited to General Records Schedule 3.1 and 3.2. After the appropriate retention period, records will be destroyed/deleted, in accordance with appropriate media sanitization procedures.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: OPM security measures are in compliance with the Federal Information Security Modernization Act of 2014, associated OMB policies, and applicable standards and guidance from the National Institute of Standards and Technology (NIST). Access to such information is limited to OPM employees, contractors, and other personnel who have an official need for access in order to perform their duties. Records are maintained in an access-controlled area, with direct access permitted to only authorized personnel. Electronic records are accessed only by authorized personnel with accounts on OPM's network. Additionally, direct access to certain information may be restricted depending on a user's role and responsibility within the organization and system. Paper records are safeguarded in accordance with appropriate laws, rules, and policies.

RECORD ACCESS PROCEDURES: Individuals seeking notification of and access to their records in this system of records may do so by submitting a request in writing to the Office of Personnel Management, Office of the General Counsel, 1900 E Street NW, Washington, DC 20415-1300 or by emailing ogcatty@opm.gov. Individuals must furnish the following information for their records to be located:

1. Full name, including any former name.
2. Date of birth.
3. Social Security Number.
4. Name and address of employing agency or retirement system.
5. Reasonable specification of the requested information.
6. The address to which the information should be sent.
7. Signature.

Individuals requesting access must also comply with OPM's Privacy Act regulations regarding verification of identity and access to records (5 CFR 297).

CONTESTING RECORD PROCEDURES: Individuals wishing to request amendment of records about themselves may do so by writing to the Office of Personnel Management, Office of the General Counsel- 1900 E Street NW, Washington, DC 20415-1300 or by emailing ogcatty@opm.gov. Requests for amendment of records should include the words "PRIVACY ACT AMENDMENT REQUEST" in capital letters at the top of the request letter; if sending the request by email, include those words in the subject line. Individuals must furnish the following information for their records to be located:

1. Full name, including any former name, and address.
2. Date of birth.
3. Social Security Number.
4. Name and address of employing agency or retirement system.
5. Precise identification of the information to be amended.

6. Signature.

Individuals requesting amendment must also comply with OPM's Privacy Act regulations regarding verification of identity and access to records (5 CFR 297).

NOTIFICATION PROCEDURES: See "Record Access Procedure."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: None.

[FR Doc. 2025-19092 Filed: 9/30/2025 8:45 am; Publication Date: 10/1/2025]