This document is scheduled to be published in the
Federal Register on 03/22/2021 and available online at
federalregister.gov/d/2021-05889, and on **govinfo.gov**

DEPARTM

Privacy Act of 1974, System of Records

AGENCY: Special Inspector General for Pandemic Recovery (SIGPR), Department of the Treasury.

ACTION: Notice of new systems of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of the Treasury proposes to establish three new systems of records within its inventory of records systems, subject to the Privacy Act of 1974 as amended. This action is necessary to meet the requirements of the Privacy Act to publish in the Federal Register notice of the existence and character of records maintained by the office.

DATES: Submit comments on or **before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. The new routine uses will be applicable on **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Comments may be submitted to the Federal eRulemaking Portal electronically at http://www.regulations.gov. Send written comments to, or request further information from:

Special Inspector General for Pandemic Recovery

2051 Jamieson Avenue, Suite 600, Alexandria Virginia 22314

ATTN: General Counsel

Comments will be made available for public inspection upon written request or by making an appointment. SIGPR will make such comments available for public inspection and copying at the above-listed location on official business days between 9 a.m. to 5 p.m. Eastern Time.

SUPPLEMENTARY INFORMATION: SIGPR was established by the Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020. SIGPR has the duty to conduct, supervise, and coordinate audits, evaluations, and investigations of the making, purchase, management, and sale of loans, loan guarantees, and other investments made by the Secretary of

the Treasury under programs established by the Secretary, as authorized by Section 4018(c) of the CARES Act, and the management by the Secretary of programs, as authorized by Section 4018(c) of the CARES Act. SIGPR's duties and responsibilities are set forth in Section 4018 of the CARES Act, and in the Inspector General Act of 1978, 5 U.S.C. app. 3. To facilitate SIGPR's audits, evaluations, investigations, and other operations to (a) promote economy, efficiency, and effectiveness in the administration of such programs; (b) prevent and detect fraud and abuse in the programs and operations within its jurisdiction; and (c) keep the head of the establishment and the Congress fully informed about problems and deficiencies relating to the administration of such programs and operations, and the necessity for and progress of corrective action, SIGPR plans to create the following systems of records:

SIGPR .420 – Audit and Evaluations Records

SIGPR .421 – Case Management System and Investigative Records

SIGPR .423 – Legal Records

Treasury has provided a report of this system of records to the Committee on Oversight and Government Reform of the U.S. House of Representatives, the Committee on Homeland Security and Governmental Affairs of the U.S. Senate, and the Office of Management and Budget (OMB), pursuant to 5 U.S.C. 552a(r) and OMB Circular A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," dated December 23, 2016.

Ryan Law,

Deputy Assistant Secretary for Privacy, Transparency, and Records.

SYSTEM NAME AND NUMBER:

Department of the Treasury, Special Inspector General for Pandemic Recovery (SIGPR) - Audit and Evaluation Records .420

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION:

Records are maintained at the Office of the Special Inspector General for Pandemic Recovery, 2051 Jamieson Avenue, Suite 600, Alexandria, VA 22314

Martinsburg Data Center, 250 Murall Drive, Kearneysville, WV 25430

Memphis Data Center, 5333 Getwell Road, Memphis, TN 38118

Other federal agencies and contractor-owned and -operated facilities

SYSTEM MANAGER(S):

Senior Advisor, Office of Audits, Special Inspector General for Pandemic Recovery, 2051 Jamieson Avenue, Suite 600, Alexandria, VA 22314

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Section 4018 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020, 5 U.S.C. App. 3, and 5 U.S.C. 301.

PURPOSE OF THE SYSTEM:

The purpose of this system is to act as a management tool for SIGPR audit and evaluation projects and personnel, and to assist in conducting accurate and timely audits and evaluations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals covered by the system are those who are the subject of, are associated with, or are witnesses referenced in, the audits and evaluations that SIGPR is authorized to conduct, supervise, and coordinate. The system may include records of auditors, evaluators, administrative support staff, and contractors.

CATEGORIES OF RECORDS IN THE SYSTEM:

SIGPR's Audit and Evaluations Records System contains information relevant and necessary to accomplish SIGPR's purpose specified in Section 4018 of the CARES Act Records in SIGPR's system are based on audits and evaluations SIGPR is authorized to conduct, supervise, and coordinate. These records may include, but are not limited to, issued audit and evaluation reports and follow-up review/reports of the implementation of any recommendation from a SIGPR audit and evaluation report, as well as working papers, which may include copies of correspondence, evidence, subpoenas, and other related documents collected, generated, or relied upon by the SIGPR Office of Audits and the Office of Evaluations during its official duties. These records may include, but are not limited to, the following:

- Individual and company names;
- Dates of birth;
- Social Security Numbers;
- Phone numbers;
- Email addresses;
- Regular mail addresses; and
- Other personally identifiable information, including employer identification numbers, system for award management numbers, taxpayer-identification numbers, bank account numbers, commercial and industry identification codes, and Dunn & Bradstreet universal numbers.

RECORD SOURCE CATEGORIES:

The records retained in SIGPR's Audit and Evaluations Records system have been and will be obtained through audits and evaluations SIGPR is authorized to conduct, supervise, and coordinate regarding the making, purchase, management, and sale of loans, loan guarantees, and other investments made by the Secretary of the Treasury under any program established by the Secretary under the CARES Act, and the management by the Secretary of any program established under the CARES Act.

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 the Privacy Act of 1974, 5 U.S.C. 552a(b), records and/or information or portions thereof maintained as part of this system may be disclosed by SIGPR outside Treasury as a routine use pursuant to 5 U.S.C. 552a(b)(3), as follows:

(1) To the United States Department of Justice ("DOJ") for the purpose of representing or providing legal advice to the Department of the Treasury and SIGPR (the Department/SIGPR) in a proceeding before a court, adjudicative body, or other administrative body before which the Department/SIGPR is authorized to appear, when such proceeding involves:

(a) The Department/SIGPR or any component thereof;

(b) Any employee of the Department/SIGPR in his or her official capacity;

(c) Any employee of the Department/SIGPR in his or her individual capacity where the Department of Justice or the Department/SIGPR has agreed to represent the employee; or

(d) The United States, when the Department/SIGPR determines that litigation is likely to affect the Department/SIGPR or any of its components, and the use of such records by the DOJ is deemed by the DOJ or the Department/SIGPR to be relevant and necessary to the litigation, provided that the disclosure is compatible with the purpose for which records were collected.

(2) To an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, background investigation, license, contract, grant, or other benefit, or if the information is relevant and necessary to a Treasury decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a

license, grant or other benefit and when the disclosure is appropriate to the proper performance of the official duties of the person making the request;

(3) To a Congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(4) To the National Archives and Records Administration Archivist (or the Archivist's designee), pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906;

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

(6) To another federal agency or federal entity, when the Department of the Treasury and/or SIGPR 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;

(7) To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which

includes criminal, civil, or regulatory violations; and

(8) To a court, magistrate, or administrative tribunal (a) in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of discovery, litigation, or settlement negotiations; (b) in response to a subpoena, where relevant or potentially relevant to a proceeding; or (c) in connection with civil and criminal law proceedings;

(9) To any source, either private or governmental, to the extent necessary to elicit information relevant to a SIGPR audit, evaluation, or investigation; and

(10) To persons engaged in conducting and reviewing internal and external peer reviews of SIGPR to ensure that adequate internal safeguards and management procedures exist within any office that had received law enforcement authorization or to ensure that auditing and evaluation standards applicable to government audits and evaluations by the Comptroller General of the United States and/or Council of the Inspectors General on Integrity and Efficiency are applied and followed.

POLICIES AND PRACTICES FOR THE STORAGE OF RECORDS:

Records may be stored electronically or on paper.

POLICIES AND PRACTICES FOR THE RETRIEVAL OF RECORDS:

Records may be retrieved by a search of any of: (1) the name of the subject of the audit, evaluation, auditor, evaluator, support staff, or contractor; (2) other personally identifiable information; or (3) case number.

POLICIES AND PRACTICES FOR THE RETENTION AND DISPOSAL OF RECORDS:

These records are currently not eligible for disposal. SIGPR is in the process of requesting approval from the National Archives and Records Administration of records disposition schedules concerning all records in this system of records.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls

have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to individuals who need to know the information to perform their official duties and have appropriate clearances.

RECORD ACCESS PROCEDURES:

See "Notification Procedures" below.

CONTESTING RECORD PROCEDURES:

See "Notification Procedures" below.

NOTIFICATION PROCEDURES:

This system of records may contain records that are exempt from the notification, access, and contesting records requirements pursuant to 5 U.S.C. 552a (j)(2) and (k)(2). However, SIGPR will consider individual requests to determine whether information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, Subpart C, Appendices A-M. Requests for information and specific guidance on where to send requests for records may be addressed to: General Counsel, SIGPR, 2051 Jamieson Avenue, Suite 600, Alexandria, VA 22314.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform to the Privacy Act regulations set forth in 31 CFR Part 1.36. You must first verify your identity, meaning that you must provide your full name, current address, date, and birthplace. You must sign your request. Your signature must either be notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. In addition, you should:

- Provide an explanation of why you believe SIGPR would have information on you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help SIGPR determine if it may have responsive records.

In addition, if your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her permission for you to access his/her records.

This information will help SIGPR to conduct an effective search and to prevent your request from being denied due to a lack of specificity or a lack of compliance with applicable regulations.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Secretary of Treasury has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a (c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g) of the Privacy Act, pursuant to 5 U.S.C. 552a (j)(2) and (k)(2). See 31 CFR 1.36. Exempt materials from other systems of records may become part of the case records in this system of records. If copies of exempt records from those other systems of records are entered into these case records, SIGPR claims the same exemptions for the records as claimed in the original primary systems of records of which they are a part.

HISTORY:

None.

SYSTEM NAME AND NUMBER:

U.S. Department of the Treasury, Special Inspector General for Pandemic Recovery (SIGPR) - Case Management System and Investigative Records .421

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records are maintained at the Special Inspector General for Pandemic Recovery, 2051 Jamieson Avenue, Suite 600, Alexandria, VA 22314

Martinsburg Data Center, 250 Murall Drive, Kearneysville, WV 25430

Memphis Data Center, 5333 Getwell Road, Memphis, TN 38118

Data Center, 300 E Street, SW, Washington, DC 20546

Other federal agencies and contractor-owned and -operated facilities

SYSTEM MANAGER(S):

Assistant Inspector General, Office of Investigations, Special Inspector General for Pandemic Recovery, 2051 Jamieson Avenue, Suite 600, Alexandria, VA 22314

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

SIGPR's authority to maintain this records system is based on Section 4018 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020, 5 U.S.C. App. 3, and 5 U.S.C. 301.

PURPOSE(S) OF THE SYSTEM:

The purpose of this Case Management System and Investigative Records system is to maintain information relevant to complaints received by SIGPR and collected as part of leads, inquiries, SIGPR proactive efforts, and investigations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals covered by the system are subjects or potential subjects of investigative activities, witnesses involved in investigative activities, and complainants/whistleblowers who contact the SIGPR Hotline during investigative activities that SIGPR is authorized to conduct, supervise, and coordinate. The system may include records of investigators, analysts, administrative support staff, and contractors.

CATEGORIES OF RECORDS IN THE SYSTEM:

The Case Management System and Investigative Records system contains information relevant and necessary to accomplish SIGPR's purpose specified in Section 4018 of the CARES Act, other relevant regulations, or Executive Orders. Specific records may include the following:

(1) Reports of investigations, which may include, but are not limited to, witness statements, affidavits, transcripts, police reports, photographs, documentation concerning requests and

approval for consensual telephone and consensual non-telephone monitoring, the subject's prior criminal record, vehicle maintenance records, medical records, accident reports, insurance policies, police reports, and other exhibits and documents collected during an investigation; (2) status and disposition information concerning a complaint or investigation, including prosecutive action and/or administrative action; (3) complaints or requests to investigate, including correspondence and verbal communications with Hotline complainants/whistleblowers; (4) subpoenas and evidence obtained in response to a subpoena; (5) evidence logs; (6) pen registers; (7) correspondence; (8) records of seized money and/or property; (9) reports of laboratory examination, photographs, and evidentiary reports; (10) digital image files of physical evidence; (11) documents generated for purposes of SIGPR's undercover activities; (12) documents pertaining to the identity of confidential informants; and (13) other documents and records collected from other government entities, private organizations, and individuals, and/or generated during the course of official duties. These records may include the following:

- Individual and company names;
- Dates of birth;
- Social Security Numbers;
- Phone numbers;
- Email addresses;
- Regular mail addresses; and
- Other personally identifiable information, including employer identification numbers, the system for award management numbers, taxpayer-identification numbers, bank account numbers, commercial and industry identification codes, and Dunn & Bradstreet universal numbers.

RECORD SOURCE CATEGORIES:

Subject individuals; individuals and organizations that have pertinent knowledge about a subject individual or corporate entity; those authorized by an individual to furnish information;

confidential informants and Federal Bureau of Investigation and other federal, state, local, and foreign entities.

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

In addition to those disclosures generally permitted under the Privacy Act of 1974, 5 U.S.C. 552a(b), records and/or information or portions thereof maintained as part of this system may be disclosed outside Treasury as a routine use pursuant to 5 U.S.C. 552a(b)(3), as follows:

(1) To the U. S. Department of Justice ("DOJ"), for the purpose of representing or providing legal advice to the U.S. Department of the Treasury (Department)/SIGPR in a proceeding before a court, adjudicative body, or other administrative body before which the Department/SIGPR is authorized to appear, when such proceeding involves:

(a) The Department/SIGPR or any component thereof;

(b) Any employee of the Department/SIGPR in his or her official capacity;

(c) Any employee of the Department/SIGPR in his or her individual capacity where the DOJ or the Department/SIGPR has agreed to represent the employee; or

(d) The United States, when the Department/SIGPR determines that litigation is likely to affect the Department/SIGPR or any of its components, and the use of such records by the DOJ is deemed by the DOJ or the Department/SIGPR to be relevant and necessary to the litigation, provided that the disclosure is compatible with the purpose for which records were collected.

(2) To an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, background investigation, license, contract, grant, or other benefit, or if the information is relevant and necessary to a Treasury decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a

license grant or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person making the request;

(3) To a Congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(4) To the National Archives and Records Administration Archivist (or the Archivist's designee) pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906;

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

(6) To another federal agency or federal entity, when the Department of the Treasury and/or SIGPR 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;

(7) To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or

in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations; and

(8) To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of discovery, litigation, or settlement negotiations, in response to a subpoena, where relevant or potentially relevant to a proceeding, or in connection with civil and criminal law proceedings;

(9) To any source, either private or governmental, to the extent necessary to elicit information relevant to a SIGPR audit, evaluation, or investigation; and

(10) To persons engaged in conducting and reviewing internal and external peer reviews of SIGPR to ensure that adequate internal safeguards and management procedures exist within any office that had received law enforcement authorization or to ensure that auditing and evaluation standards applicable to government audits and evaluations by the Comptroller General of the United States and/or Council of the Inspectors General on Integrity and Efficiency are applied and followed.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records may be stored electronically or on paper.

POLICES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by name, personally identifiable information, and/or case number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

These records are currently not eligible for disposal. SIGPR is in the process of requesting approval from the National Archives and Records Administration of records disposition schedules concerning all records in this system of records.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies. Records security is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in SIGPR's records.

SIGPR's safeguards ensure that its records system and applications operate effectively and provide appropriate confidentiality, integrity, and availability through cost-effective management, personnel, operational, and technical controls. The safeguards further ensure the security and confidentiality of the records in its system and help protect against anticipated threats or hazards. All individuals granted access to SIGPR's system of records need to know the information to perform their official duties and have the appropriate training and clearances.

RECORD ACCESS PROCEDURES:

See "Notification Procedures" below.

CONTESTING RECORD PROCEDURES:

See "Notification Procedures" below.

NOTIFICATION PROCEDURE:

This system of records may contain records that are exempt from the notification, access, and contesting records requirements pursuant to 5 U.S.C. 552a (j)(2) and (k)(2). However, SIGPR will consider individual requests to determine whether information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, Subpart C, Appendices A-M. Requests for information and specific guidance on where to send requests for records may be addressed to: General Counsel, SIGPR, 2051 Jamieson Avenue, Suite 600, Alexandria, VA 22314.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 31 CFR Part 1.36. You must first verify your identity, meaning that you must provide your full name, current address, date, and birthplace. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. In addition, you should:

- Provide an explanation of why you believe SIGPR would have information on you;

- Specify when you believe the records would have been created; and
- Provide any other information that will help SIGPR determine if it may have responsive records.

In addition, if your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her permission for you to access his/her records.

This information will help SIGPR to conduct an effective search and to prevent your request from being denied due to a lack of specificity or a lack of compliance with applicable regulations.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Secretary of Treasury has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a (c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2) and (k)(2). Exempt materials from other systems of records may become part of the case records in this system of records. If copies of exempt records from those other systems of records are entered into these case records, SIGPR claims the same exemptions for the records as claimed in the original primary systems of records of which they are a part.

HISTORY:

None.

SYSTEM NAME AND NUMBER:

Department of the Treasury, Special Inspector General for Pandemic Recovery (SIGPR) - SIGPR Legal Records .423

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records are maintained at the Special Inspector General for Pandemic Recovery, 2051 Jamieson Avenue, Suite 600, Alexandria, VA 22314

Martinsburg Data Center, 250 Murall Drive, Kearneysville, WV 25430

Memphis Data Center, 5333 Getwell Road, Memphis, TN 38118

Other federal agencies and contractor-owned and -operated facilities

SYSTEM MANAGER(S):

Office of General Counsel, Special Inspector General for Pandemic Recovery

2051 Jamieson Avenue, Suite 600, Alexandria, VA 22314

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Section 4018 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020, 5 U.S.C. App. 3, and 5 U.S.C. 301.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to: (1) assist SIGPR attorneys in providing legal advice to the agency on a wide variety of legal issues; (2) collect information about any individual who is, or will be, in litigation with the agency, as well as related to the attorneys representing the plaintiff(s)' and defendant(s)' response to claims of employees, former employees, or other individuals; (3) assist in settlement of claims against the government, and (4) represent SIGPR in litigation.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Persons identified in files maintained by the SIGPR Office of General Counsel, which include attorneys, litigants, and other claimants against SIGPR and its contractors; persons who are the subject of claims by SIGPR and persons against whom SIGPR considered asserting claims; witnesses and third parties to claims or litigation; SIGPR's contractors and potential contractors; SIGPR employees subject to garnishment or assignments; and SIGPR employees and contractors who use Alternate Dispute Resolution (ADR).

CATEGORIES OF RECORDS IN THE SYSTEM:

Records concerning legal matters include (1) materials assigned to the SIGPR Office of General Counsel and that are related to litigation and all other claims against or by SIGPR and its contractors; (2) SIGPR contracts and related materials; and (3) materials pertaining to ADR. Litigation and claim records may include, but are not limited to, correspondence and pleadings (such as complaints, answers, counterclaims, motions, depositions, court orders and briefs). Records in this system include, but are not limited to, documents such as accident reports, inspection reports, investigation reports, audit reports, evaluation reports, personnel files, contracts, consultant agreements, reports about criminal matters of interest to SIGPR, Personnel Security Review Board documents, medical records, photographs, telephone records, correspondence, memoranda, and other related documents. These records may include materials that establish or document key information related to individuals or entities. such as:

- Individual and company names;
- Dates of birth;
- Social Security Numbers;
- Phone numbers;
- Email addresses;
- Regular mail addresses; and
- Other personal identifiable information, including employer identification numbers, system for award management numbers, taxpayer identification numbers, bank account numbers, commercial and industry identification codes, and Dunn & Bradstreet universal numbers.

RECORD SOURCE CATEGORIES:

Sources of records include subject individuals, inspection reports, other agencies, SIGPR Office of General Counsel attorneys, other agency officers and staff, contractors, investigators, evaluators, auditors, and any person who may provide data, materials or information that SIGPR

Office of General Counsel is authorized to collect concerning potential or actual litigation or claims concerning SIGPR or a SIGPR employee.

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

In addition to those disclosures generally permitted under the Privacy Act of 1974, 5 U.S.C. 552a(b), records and/or information, or portions thereof, maintained as part of this system may be disclosed outside Treasury as a routine use pursuant to 5 U.S.C. 552a(b)(3), as follows:

(1) To the United States Department of Justice ("DOJ"), for the purpose of representing or providing legal advice to the U.S. Department of Treasury (Department)/SIGPR in a proceeding before a court, adjudicative body, or other administrative body before which the Department/SIGPR is authorized to appear, when such proceeding involves:

(a) The Department/SIGPR or any component thereof;

(b) Any employee of the Department/SIGPR in his or her official capacity;

(c) Any employee of the Department/SIGPR in his or her individual capacity where DOJ or the Department/SIGPR has agreed to represent the employee; or

(d) The United States, when the Department/SIGPR determines that litigation is likely to affect the Department/SIGPR or any of its components, and the use of such records by the DOJ is deemed by the DOJ or the Department/SIGPR to be relevant and necessary to the litigation, provided that the disclosure is compatible with the purpose for which records were collected.

(2) To an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, background investigation, license, contract, grant, or other benefit, or if the information is relevant and necessary to a Treasury decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a

license, grant, or other benefit, and when disclosure is appropriate to the proper performance of the official duties of the person making the request;

(3) To a Congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(4) To the National Archives and Records Administration Archivist (or the Archivist's designee) pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906;

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

(6) To another federal agency or federal entity, when the Department of the Treasury and/or SIGPR 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; and

(7) To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or

in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations; and

(8) To a court, magistrate, or administrative tribunal in the course of presenting evidence or filing pleadings; to opposing counsel or witnesses in the course of discovery, litigation, or settlement negotiations, or in response to a subpoena, or where relevant or potentially relevant to a proceeding or in connection with civil or criminal law proceedings.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records may be stored electronically and/or as paper records.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrievable by name, case name, claim name, or assigned identifying number, in accordance with an appropriate classification system.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

These records are currently not eligible for disposal. SIGPR is in the process of requesting approval from the National Archives and Records Administration of records disposition schedules concerning all records in this system of records.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies. Records security is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in SIGPR's records. SIGPR's safeguards ensure that its records system and applications operate effectively and provide appropriate confidentiality, integrity, and availability through cost-effective management, personnel, operational, and technical controls. The safeguards further ensure the security and confidentiality of the records in its system and help protect against anticipated threats or hazards. All individuals granted access to SIGPR's records system need to know the information to perform their official duties and have the appropriate training and clearances.

RECORD ACCESS PROCEDURES:

See “Notification Procedures” below.

CONTESTING RECORD PROCEDURES:

See “Notification Procedures” below.

NOTIFICATION PROCEDURES:

This system of records may contain records that are exempt from the notification, access, and contesting records requirements pursuant to 5 U.S.C. 552a (j)(2) and (k)(2). However, SIGPR will consider individual requests to determine whether information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing at 31 CFR part 1, Subpart C, Appendices A-M. Requests for information and specific guidance on where to send requests for records may be addressed to: General Counsel, SIGPR, 2051 Jamieson Avenue, Suite 600, Alexandria, VA 22314.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 31 CFR Part 1.36. You must first verify your identity, meaning that you must provide your full name, current address, date of birth, and birthplace. You must sign your request, and your signature must be either notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. In addition, you must:

- Provide an explanation of why you believe SIGPR would have information on you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help SIGPR determine if it may have responsive records.

If you are requesting records about another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

This information will help SIGPR to conduct an effective search and to prevent your request from being denied due to a lack of specificity or a lack of compliance with applicable regulations.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Secretary of Treasury has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2) and (k)(2). See 5 CFR part 9301. Exempt materials from other systems of records may become part of the case records in this system of records. If copies of exempt records from those other systems of records are entered into these case records, SIGPR claims the same exemptions for the records as claimed in the original primary systems of records of which they are a part.

HISTORY:

None.

[FR Doc. 2021-05889 Filed: 3/19/2021 8:45 am; Publication Date: 3/22/2021]