Privacy Impact Assessment
for the

Case Logging, Enforcement & Activity Reporting System (CLEAR)

October 23, 2018

Contact Point
Gopala Seelamneni
Chief Information Technology Officer
Office of the Inspector General

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer

Abstract

The Office of the Inspector General (OIG) is an independent office within the U.S. Office of Personnel Management (OPM) and has a statutory mission to provide objective oversight of OPM programs and operations. The Case Logging, Enforcement and Activity Reporting (CLEAR) system is administered and operated by the OIG Office of Investigations. CLEAR is used to track, manage, and report on law enforcement investigations and activities conducted by OIG staff. This Privacy Impact Assessment (PIA) is required because the CLEAR system maintains personal information in identifiable form.

Overview

The OIG is an independent and objective oversight office within OPM. In accordance with the Inspector General Act of 1978, as amended (IG Act), 5 U.S.C. app., the OIG conducts and supervises audits, investigations, and evaluations relating to OPM programs and operations. The OIG investigates potential violations of law, rules, or regulations; incidents of mismanagement, gross waste of funds, or abuse of authority; and matters constituting a substantial and specific danger to the public health and safety; and supports or is otherwise involved in civil, criminal, and administrative proceedings related thereto. The OIG conducts investigations jointly and in coordination with the U.S. Department of Justice (DOJ) and other Federal, state, and local law enforcement agencies.

Information concerning suspected or potential fraud, waste, and abuse related to OPM programs and operations may be reported by OPM or other Federal employees, Federal contractors, other Federal, state, or local agencies, or members of the general public. The OIG also uses data analytics to identify potential fraud impacting OPM programs and operations, and participates in a variety of Federal and state law enforcement task forces across the country.

The CLEAR system provides foundational information for case processing, management, and reporting functions related to the OIG's law enforcement investigations and activities. CLEAR is a web-based, browser-based application deployed on an application server managed by a FedRAMP-

certified vendor. The system supports investigative case management tracking, while providing configuration capabilities which allow development of data structures, forms, reports, and workflow to meet OIG's case tracking requirements. CLEAR also allows OIG criminal investigators and other investigative staff to create case records and input information or attach electronic documentation as appropriate to facilitate investigative activities.

The application is managed and operated solely by OIG staff. Within the OIG, information in CLEAR is further restricted so as to permit OIG employees access only to information required in the performance of the employees' duties. Reports from the system are used internally by OIG management to track, evaluate, and manage program operations, and as a basis for reporting investigative results and statistics internally and externally. Limited reports on investigative activities are shared as required by law or as otherwise appropriate to support the OIG's mission, including with the U.S. Congress, DOJ, other law enforcement partners, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The IG Act, 5 U.S.C. app., establishes the OIG and sets forth its purpose, duties, and authorities. Most pertinently, the IG Act authorizes the OIG, in the course of carrying out its statutory responsibilities, "to have timely access to all records, reports, audits, reviews, documents, papers, recommendations, or other materials available to [OPM] which relate to [OPM] programs and operations," (5 U.S.C. app.§ 6(a)(1)); "to make such investigations and reports relating to the administration of the programs and operations of the applicable establishment" as the Inspector General determines to be "necessary or desirable," (5 U.S.C. app.§ 6(a)(2)); "to request such information or assistance as may be necessary . . . from any Federal, State, or local governmental agency or unit thereof," (5 U.S.C. app. § 6(a)(3)); "to require by subpoena the production of all information, documents, reports, answers, records, accounts, papers, and other data in any medium (including electronically stored information), as well as any tangible thing and documentary evidence," (5 U.S.C. app. § 6(a)(4)); and

"to administer to or take from any person an oath, affirmation, or affidavit," (5 U.S.C. app.§ 6(a)(5)).

Executive Order 9397, as amended by Executive Order 13478, permits the collection and use of Social Security Numbers (SSNs).

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The OPM/CENTRAL-4 Inspector General Investigations Case Files SORN applies to information maintained in this system. 55 Fed. Reg. 3802 (Feb. 5, 1990); 60 Fed. Reg. 63075 (Dec. 8, 1995); 80 Fed. Reg. 74815 (Nov. 30, 2015).

1.3. Has a system security plan been completed for the information system(s) supporting the project?

CLEAR has a system security plan that was last updated in June 2018. CLEAR was granted an Authority to Operate (ATO) on August 27, 2018.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. N1-478-08-001, OPM Inspector General Records.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The PRA does "not apply to the collection of information during the conduct of an audit, investigation, inspection, evaluation, or other review conducted by . . . any Office of Inspector General . . . ." The IG Act, 5. U.S.C. app. § 6(k).

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

CLEAR contains investigative, personnel (support), and administrative data collected by the OIG. The system includes numerous types of information about individuals, including name, address, SSN, telephone number, e-mail address, photograph, or other unique identifying number, code, or

characteristic, gender, race, date of birth, place of birth, geographic indicator, license number, vehicle identifier including license plate, and other descriptors. Other information about individuals that may be in CLEAR includes financial account numbers, and medical, educational, or personnel records.

Information contained in CLEAR may be about U.S. citizens, current or former Federal employees, Federal contractors and contractor employees, complainants, witnesses, subject matter experts, law enforcement partners, and other persons relating to OPM programs and operations. Information may be about living or deceased individuals.

2.2. What are the sources of the information and how is the information collected for the project?

The sources of information in CLEAR include direct collection from the individual record subjects, complainants, or third parties with information pertinent to OIG investigative activities (including witnesses and other entities having some relationship with the record subject); the files of OPM offices and their systems of records; other Federal, state, and local agencies; and non-government record sources; including commercial databases that provide public records search and link analysis capabilities.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

While CLEAR does not directly connect with any commercial or publicly available data sources, OIG investigative staff utilize commercial and publicly available data sources in the course of their investigative activities. These data sources may be used to obtain information that is used to corroborate evidence and to identify and locate potential subjects, witnesses, and record sources. The source of the information is generally noted when the incorporation of the information is recorded pursuant to standard OIG procedures regarding the evidential documenting of investigative activities.

2.4. Discuss how accuracy of the data is ensured.

Information obtained in the course of OIG investigative activities is verified through the investigative process; information is subject to evaluation and

scrutiny by OIG investigative staff and verified against information collected from other records sources. Accuracy is further ensured through the use of supervisory reviews of investigative activity.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the information in CLEAR will be inaccurate or incomplete.

Mitigation: This risk is mitigated by standard investigative procedures whereby OIG investigative staff validates information obtained by verifying the information against other records sources. These procedures are reinforced by internal policies, external guidelines (including the CIGIE Quality Standards for Investigations), and supervisory reviews of investigative activities.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

Information is maintained in CLEAR in order to allow the OIG to meet its statutory responsibility to provide independent and objective oversight of OPM, including by conducting criminal, civil, and administrative investigations related to OPM programs and operations. Information collected and maintained in the system is used to detect and investigate activity constituting a potential violation of law, rule, or regulation; or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety; and to support the pursuit of criminal, civil, or administrative actions for such activities, as appropriate. Information is also used by OIG management to track, evaluate, and manage program operations, and as a basis for reporting investigative results and statistics internally and externally. SSNs are used to confirm individuals' identities and to facilitate certain law enforcement requests.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

CLEAR employs a search function that enables OIG staff to identify commonalities between different investigative activities, thereby allowing for the identification and consolidation of duplicative activities and the efficient assignment of duties. CLEAR is also capable of producing reports, which are used internally to track, evaluate, and manage OIG program operations and externally to convey OIG investigative statistics as required by law or as otherwise appropriate to support the OIG's mission.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

No. Access to CLEAR is limited to OIG personnel only. No other OPM offices or programs have access to the system's information.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that an authorized person may access the information for an unauthorized purpose and that PII may be accessed or used inappropriately or in a manner not consistent with the original program's purpose or the user's specific mission area and authority.

Mitigation: This risk is mitigated by limiting access according to user roles and work assignments, by documenting disclosures, and by the use of built-in audit logs that document users' access to information. This risk is further mitigated by reviews by supervisory investigative staff. Additionally, all employees who are authorized to access CLEAR are required to have as a prerequisite certain OPM OIG training, including an ethics briefing. Users are also required to comply with and acknowledge OIG-specific rules of behavior to access CLEAR and other OIG IT resources.

Privacy Risk: There is a risk that individuals who do not have a need to know the information in the investigative process will access and use the information for unauthorized purposes.

Mitigation: This risk is mitigated by limiting access according to user roles and work assignments, by documenting disclosures, and by the use of built-in audit logs that document users' access to information. These logs are checked to ensure that the system is not accessed inappropriately. User access is based on express permission and the OPM OIG limits access to those employees with a need to know basis.

There are also multiple layers of physical and IT protections that are used to safeguard the information in CLEAR. Physical security on the premises ensures that only authorized individuals have access to OIG offices. Firewalls and data encryption methods ensure the data can only be accessed by authorized OIG personnel. Limiting access to only those cases for which there is a need to know further prevents against unauthorized access or use.

Section 4.0. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Notice is provided through this PIA and the SORN identified in section 1.2. Notice is also provided with respect to certain categories of information collected from CLEAR users, including administrative and personnel (support) records.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Insofar as information is obtained directly from the record subject, individuals may have the opportunity to decline to provide information. OIG criminal investigators are trained as to investigative subjects' rights and obligations when responding to OIG inquiries, and the OIG has policies in place to ensure that subjects are made aware of those rights, as appropriate.

In instances where information is obtained by the OIG from other record sources (including witnesses, commercial or publicly available databases, and Federal systems of records) the individual generally is not provided the opportunity to consent or object to the OIG's collection. Providing individuals additional specific notice at the point of collection of information could negatively impact the investigative activities of the OIG by, for

example, alerting the subjects of criminal investigations as to the Government's prosecutorial strategies or the nature of evidence collected.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not receive adequate notice concerning how their information is used in CLEAR and individuals may not be aware that the system collects and uses their information.

Mitigation: This risk is partially mitigated with the notification regarding the collection, maintenance, and use of information contained in this system is provided through publication of this PIA and the SORN listed in section 1.2, above. Individuals wishing to learn whether this system contains information about them may contact the system manager. However, notice and consent may not be possible in certain circumstances, due to the risk of alerting the subjects of investigations as to the Government's prosecutorial strategies or the nature of evidence collected, which could inhibit or detrimentally affect the OIG's capacity to detect unlawful activity.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

Information in CLEAR is retained in accordance with the NARA retention schedule noted in section 1.4, above. Files associated with a particular investigative activity are maintained in the system for five years after the investigative activity and any associated litigation is complete, and retained on-site for an additional ten years, after which they are destroyed.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information may be kept longer than is necessary to meet the business need for which it was collected.

Mitigation: This risk is mitigated by adherence to the established retention schedule and documented guidance from NARA, which clearly defines retention requirements by record type and agency.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Any information sharing from CLEAR comports with the statutory responsibilities of the IG Act, 5 U.S.C. app., which authorizes the audit, investigation, and evaluation of OPM programs and operations as well as the collection of related information.

Information in CLEAR is regularly shared with DOJ pursuant to the IG Act, 5 U.S.C. app. § 4(d), which requires the OIG to "report expeditiously to the Attorney General whenever the Inspector General has reasonable grounds to believe there has been a violation of Federal criminal law;" and to otherwise support the criminal and civil prosecution of violations of law impacting or relating to OPM programs and operations.

Information is also shared, as appropriate, with other Federal, state, and local agencies (including other Federal Offices of Inspectors General) pursuant to joint investigations involving OPM programs and operations, or where the OPM OIG becomes aware of an indication of a violation or potential violation of law falling within the jurisdiction of the agency.

Information in CLEAR is also shared in order to comply with various reporting requirements, including the annual report required by the Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority and the semiannual report to Congress required by the IG Act, 5 U.S.C. app. § 5.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Insofar as the information sharing described in section 6.1 implicates Privacy Act-protected information and is not otherwise permitted by the conditions for disclosure enumerated at 5 U.S.C. § 552a(b), it is permitted by the routine uses listed in the SORN for OPM/CENTRAL-4, Inspector General Investigations Case Files, or incorporated by reference from the Prefatory Statement of Routine Uses for OPM's Internal and Central Systems of Records. The predominant routine uses include:

- For Law Enforcement Purposes--To disclose pertinent information to the appropriate Federal, State, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where OPM becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.
- For Litigation--To disclose information to the Department of Justice, or in a proceeding before a court, adjudicative body, or other administrative body before which OPM is authorized to appear, when: (1) OPM, or any component thereof; or (2) Any employee of OPM in his or her official capacity; or (3) Any employee of OPM in his or her individual capacity where the Department of Justice or OPM has agreed to represent the employee; or (4) The United States, when 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 or OPM is deemed by OPM to be relevant and necessary to the litigation provided, however, that the disclosure is compatible with the purpose for which records were collected.
- For the Merit Systems Protection Board--To disclose information to officials of the Merit Systems Protection Board or the Office of the Special Counsel, when requested in connection with appeals, special studies of the civil service and other merit systems, review of OPM rules and regulations, investigations of alleged or possible prohibited personnel practices, and such other functions, e.g., as promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.
- To any source from which information is requested in the course of an investigation, to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.

6.3. Does the project place limitations on re-dissemination?

Disclosures from CLEAR may be accompanied by a notice advising against further release without the prior authorization of the OPM OIG.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

Disclosures outside the OIG are recorded in CLEAR pursuant to the OIG's standard investigative procedures, which require OIG investigative staff to timely document actions taken pursuant to an investigative activity within the CLEAR entry associated with that investigative activity. Records of disclosures note the information disclosed, the individual effecting the disclosure, the entity to whom the information was disclosed, and the date on which the disclosure was made.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information in OIG CLEAR will be shared with a third party and used or disseminated for a purpose that is not consistent with the purpose for which it was collected.

Mitigation: This risk is mitigated by the implementation of internal OPM and OIG guidance and policies on the release of information, and by limiting releases to the extent necessary to facilitate OPM OIG investigative activities; to support civil, criminal, or administrative prosecutions resulting from or related to OIG investigative activities; and to meet reporting requirements. This risk is further mitigated by limiting OIG employees' access to information in CLEAR according to the duties of their positions.

Section 7.0. Redress

7.1. What are the procedures that allow individuals to access their information?

There is limited access to investigative information and certain records in CLEAR because they have been exempted from the access (including access to an accounting of disclosures) provisions of the Privacy Act, 5 U.S.C. § 552a(c)(3) and (d). 5 C.F.R. § 297.501(b)(1). Individuals seeking to access records in CLEAR pertaining to themselves may contact the CLEAR system manager, as noted in the SORN for OPM/CENTRAL-4, Inspector General Investigations Case Files.

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

There is limited opportunity to amend investigative information and certain records in CLEAR because they have been exempted from the amendment provisions of the Privacy Act, 5 U.S.C. § 552a(d). 5 C.F.R. § 297.501(b). Individuals seeking to amend records in CLEAR pertaining to themselves may contact the CLEAR system manager, as noted in the SORN for OPM/CENTRAL-4, Inspector General Investigations Case Files.

7.3. How does the project notify individuals about the procedures for correcting their information?

The procedures for individuals to correct information are described in the SORN for OPM/CENTRAL-4, Inspector General Investigations Case Files and in this PIA.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not have the opportunity to access or amend inaccurate information maintained by other agencies and submitted to CLEAR.

Mitigation: This risk cannot be completely mitigated since providing individuals the opportunity to access or amend information in CLEAR could negatively impact the investigative activities of the OIG by, for example, alerting the subjects of criminal investigations as to the Government's prosecutorial strategies or the nature of evidence collected. Further, the accuracy or relevance of information obtained during the course of an investigation may not be readily apparent at the time of collection. Accordingly, allowing the premature amendment of information could inhibit or detrimentally affect the OIG's capacity to detect unlawful activity. However, this risk is partially mitigated by the publication of instructions on the OPM website, in this PIA, and in the SORN listed in section 1.2, above, to inform individuals about how to request access to and amendment of their records, notwithstanding that certain records in this system have been exempted from the access and amendment provisions of the Privacy Act.

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

CLEAR user access is based on express permission and the OPM OIG limits access to information to those employees with a need to know the information in the performance of their duties. Users are assigned roles, which have access privileges according to the user's duties and assigned investigative activities. There are also multiple layers of physical and IT protections that are used to safeguard the information in CLEAR. Physical security on the premises ensures that only authorized individuals have unaccompanied access to OIG offices. Firewalls and data encryption methods ensure the data can only be accessed by authorized OIG personnel.

CLEAR employs built-in audit logs that document users' access to information. These logs are checked to ensure that the system is not accessed inappropriately.

Adherence to the stated practices in this PIA is further ensured by internal OIG policies describing employees' responsibilities with respect to the maintenance and use of information, and by the provision of privacy training described in section 8.2, below. Additionally, not less than once every three years, the OIG Office of Investigations is subject to peer review by another Federal Office of Inspector General, which evaluates adherence to the CIGIE Quality Standards for Investigations. OIG records management practices may be assessed as part of this triennial peer review, the results of which are made publicly available on the OIG's website.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM employees receive annual training on IT security and privacy awareness, which includes instruction on the proper handling of PII. All employees who are authorized to access CLEAR are required to have as a prerequisite certain OIG training, including an ethics briefing. Users are further required to learn and acknowledge specific rules of behavior governing access to CLEAR and other OIG IT resources. Once granted access to CLEAR, employees are provided additional training on their user roles.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

CLEAR user access is based on express permission and access to information is limited to those OPM OIG employees with a need to know the information in the performance of their duties. Access is limited solely to OIG employees, who are granted access to CLEAR and assigned roles by system administrators only after receiving the instruction described in section 8.2, above. CLEAR users' access is further limited within the system to information pertaining to their assigned duties during the pendency of those duties. Firewalls and data encryption methods ensure the data can be accessed by authorized OIG personnel only.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

The OIG does not have any information sharing agreements, nor is access to CLEAR granted to non-OIG employees. Any new uses of the information, memoranda of understanding, information sharing agreements, or provisions of access would be reviewed by OIG senior level management, to ensure that the contemplated change aligns with the OIG's mission, that necessary technical safeguards are in place, and that all legal requirements are met.

Responsible Officials

Gopala Seelamneni
Chief Information Technology Officer
Office of the Inspector General
U.S. Office of Personnel Management

Approval Signatures

Signed copy on file with OPM's Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer
U.S. Office of Personnel Management