1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld Bureau of Administration Information Sharing Services Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: September 15, 2008

(b) Name of system: Office of Investigations-Case Management System

(c) System acronym: OIG-CMS

(d) IT Asset Baseline (ITAB) number: 387

(e) System description: (Briefly describe scope, purpose, and major functions):

The Office of Investigations operates the Office of Inspector General (OIG) Hotline, which provides an effective, direct channel for employees and contract personnel, as well as private citizens, to report incidents of waste, fraud, abuse, and mismanagement to the OIG. The OIG Case Management System allows the OIG to manage and track the OIG Hotline, preliminary and case statistical data for OIG Special Agent investigations and reporting.

(f) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security re-certification

(g) Explanation of modification (if applicable): N/A

(h) Date of previous PIA (if applicable): November 2007

3. Characterization of the Information

The system:

- ☐ does NOT contain PII. If this is the case, you must only complete Section 13.
- ☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

- Names;
- Dates of birth; and
- Social security numbers

Sources of information are U.S. Government employees, contractor or private citizens.

b. How is the information collected?

Information is collected through hotline submissions via phone, online, cables or by interviews with the person who is alleging or has witnessed wrong doing.

c. Why is the information collected and maintained?

The Office of Inspector General Hotline is a clearinghouse for receiving and handling allegations regarding fraud, waste, abuse, mismanagement or misconduct affecting the Department of State (DOS) and the Broadcasting Board of Governors (BBG) programs and operations. The information is collected for investigative and reporting purposes.

d. How will the information be checked for accuracy?

The information entered into the system concerns allegations of wrong doing. The source of information is responsible for entering only information that is factual and accurate. The OIG investigates the information given to validate its credibility.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- The Foreign Service Act of 1980 (22 U.S.C. 3901) in accordance with the Department of State Authorization Act for Fiscal Year 1986; and
- Inspector General Act of 1978 (5 U.S.C. Appendix 3).

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they are mitigated.

The privacy risks are low. The minimum amount of PII is collected to satisfy the purpose of this system. Any personnel information disclosed during an investigation is confidential.

4. Uses of the Information

a. Describe all uses of the information.

The information will be used by the OIG to promptly review allegations of wrong doing.

b. What types of methods are used to analyze the data? What new information may be produced?

Any new information produced is an allegation of waste, fraud, abuse or misconduct. An OIG special agent will be assigned to investigate the allegation. Individuals will be informed if they are the subject of a criminal investigation or are being contacted as a witness.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

Information from other Federal Agency databases will be use by OIG to promptly investigate allegations of wrong doing.

d. Is the system a contractor used and owned system?

OIG-CMS is a U.S. Government system maintained by cleared government employees. All employees undergo an annual security briefing and Privacy Act briefing.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Access to the OIG-CMS requires a unique user account assigned to Investigation and IT administration staff by the OIG. Each authorized user must first sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed for the performance of his or her official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g., curiosity browsing).

5. Retention

a. How long is information retained?

Investigative reports and files containing information or allegations which are of an investigative nature but do not relate to specific investigations are destroyed when five years old. All other investigation files are cutoff inactive at end of a year and destroyed when 10 year old.

b. Privacy Impact Analysis: Discuss the risk associated with the duration that data is retained and how those risks are mitigated.

Regular backups are performed and recovery procedures are in place for OIG-CMS. All records containing personal information are maintained in secured file cabinets or in restricted areas, access to which is limited to authorized personnel only. Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached their retention period, they are immediately retired or destroyed in accordance with the National Archive and Records Administration (NARA).

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

Status reports on investigation can be shared with Department managers if they do not jeopardize the integrity of the investigation or unduly infringe on the privacy rights of the accused.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

The information is only disclosed to Department managers in paper format only and requires that a change of custody receipt be signed. Only authorized cleared OIG users have access to the system. This information will not be disclosed if it jeopardizes the integrity of the investigation or unduly infringe on the privacy rights of the accused.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

There are no privacy risks associated with the internal sharing of information.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

The information can be shared with the Department of Justice and host country, state or local authorities, if there is evidence of criminal misconduct. Noncriminal matter may be disclosed to the Director General of Human Resources (DGHR).

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Information is shared outside of the Department in paper format only. A receipt for change of custody is maintained for information that is shared.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The OIG conducts investigations according to investigative procedures established by the professional community, which include reviews of relevant files and documentation and interviews with and written statements from complainants, witnesses, technical experts, and subjects of inquiries. The information shared with external entities is in accordance with statutory authority.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

State-53 Records of the Inspector General and Automated Individual Cross-Reference System

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems):

a. Is notice provided to the individual prior to collection of their information?

Individuals voluntarily submit information to the hotline on alleged wrong doings and are automatically granted confidentiality on any complaints made to the OIG. An employee will be advised whether they are the subject or witness of a criminal investigation prior to collection.

b. Do individuals have the opportunity and/or right to decline to provide information?

Individuals who submit information to the hotline may choose to remain anoymous. This, however, may limit the ability for the OIG to conduct a complete investigation into the matter and may result in closure due to insufficient information. Individuals who are subjects of a criminal investigative can decline to provide information.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Because the case involves the possible violation of laws, regulations, code of conduct and ethnics, the individual does not have the right to consent or specify the uses of the information collected.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The notice offered is reasonable and adequate in relation to the system's purposes and uses.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Procedures for notification and redress are published in the system of record State-53, Records of the Inspector General and Automated Individual Cross-Reference System and rules published at 22 CFR 171.31. Individuals who want to gain access to amend their record or have reason to believe that the records of the Inspector General and Automated Individual Cross-Reference System might contain information pertaining to them, should write to the Director, Office of Information Programs and Services (A/ISS/IPS), SA-2, Department of State, 515 22nd Street, Washington DC 20522-8001. The individual must specify that he or she wishes the Records of the Inspector General and Automated Individual Cross-Reference System to be checked. At a minimum, the individual should include: name, date and place of birth, current mailing address and zip code, and signature.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notification and redress mechanisms offered to individual are reasonable and adequate in relation to the system's purpose and uses.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Internal access to OIG-CMS is limited to authorized Department of State OIG Investigation staff having a need for the system in the performance of their official duties. All users maintain a least a SECRET security clearance level in order to gain access to the Department's unclassified computer network. To access the system, the individual must first be an authorized user of the Department's unclassified computer network. Access to OIG-CMS requires a unique user account assigned to only Investigation and IT administration staff by the OIG. Each prospective authorized user must first sign a user access agreement before being given a user account. The individual's supervisor

must sign the agreement certifying that access is needed in order for the individual to perform his or her official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the information system security officer (ISSO) prior to assigning the individual a logon. The level of access for the user restricts the data that may be seen and the degree to which data may be modified. A system use notification ("warning banner") is displayed before logon is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

b. What privacy orientation or training for the system is provided authorized users?

All users are required to undergo computer security and privacy awareness training prior to being given access to the system and must complete refresher training yearly in order to retain access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

There re no expected residual risks.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

No technologies commonly considered to elevate privacy risk are employed.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risks.

Not applicable.

12. Security

What is the security certification and accreditation (C&A) status of the system?

OIG-CMS was certified and accredited for use by the Department in November 2007.