

## 1. Contact Information

**Department of State Privacy Coordinator**

Sheryl Walter  
Bureau of Administration  
Global Information Services  
Office of Information Programs and Services

## 2. System Information

- (a) Date PIA was completed: June 2013
- (b) Name of system: Office of Inspector General-Investigative Management System
- (c) System acronym: OIG-IMS
- (d) IT Asset Baseline (ITAB) number: 387
- (e) System description:

The Office of Investigations (OIG/INV) operates the Department of State Office of Inspector General (OIG) Hotline, which provides an effective and direct channel for employees, contract personnel, and private citizens to report allegations of waste, fraud, abuse, mismanagement, and misconduct. OIG-IMS allows INV to compile, manage, track, and investigate Hotline allegations (and investigative records received through other channels) as electronic case records assembled by OIG/INV special agents, paper versions of Reports of Investigation (ROIs), and to produce statistical data for official reporting purposes.
- (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:

This PIA is updated to describe OIG/INV's transition to a case management system operated by the National Aeronautics and Space Administration Office of Inspector General (NASA-OIG) on behalf of the Department of State and other Federal agencies.
- (h) Date of previous PIA: April 2011.

## 3. Characterization of the Information

The system:

- does NOT contain PII.
- does contain PII.

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

The following elements of PII exist in records compiled in OIG-IMS:

- Person name
- Date of birth
- Social Security number, and
- Passport number

The sources of information containing PII are U.S. Government employees, contractors, or private citizens who are subjects of an investigation, third parties, or witnesses. Each of these sources might provide any or all of the PII elements listed above, depending on the specifics of each investigation.

**b. How is the information collected?**

Information is submitted to the OIG Hotline via phone, online (at <http://oig.state.gov/hotline/130564.htm>), Diplomatic cable, or post office box, or by interviews with a subject, third party complainant, or witness. Submitted and collected information is entered into OIG-IMS by OIG personnel with proper access to OIG-IMS.

**c. Why is the information collected and maintained?**

OIG-IMS supports OIG/INV's effective and accurate handling of allegations of fraud, waste, abuse, mismanagement, or misconduct affecting Department of State (DOS), Broadcasting Board of Governors (BBG), and U.S. Section of the International Boundary and Water Commission (IBWC) programs and operations. The information is collected and maintained for investigative and reporting purposes.

**d. How will the information be checked for accuracy?**

The information entered in OIG-IMS concerns allegations of wrongdoing. OIG/INV staff members are responsible for entering information that is reasonably considered to be factual and accurate into the system. OIG/INV investigates this information to validate its credibility and accuracy during the course of an official investigation. Effective investigations require the compilation of information that eventually may not prove relevant to a case. Such information may be kept to provide leads for appropriate law enforcement actions and to establish patterns of activity that might relate to OIG's jurisdiction or that of other agencies. The factual correctness of investigative records in the eyes of the law may, at times, only be fully established through formal court proceedings.

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

- Section 209 of the Foreign Service Act of 1980, as amended (22 U.S.C. § 3929);
- Inspector General Act of 1978, as amended (5 U.S.C. app.); and

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

Privacy risks are low. The minimum amount of PII is collected to satisfy the statutory purpose for its collection. Any personal information disclosed to another federal, state, or local agency or office in the furtherance of an investigation is accompanied by

notification that it is to be used for official purposes only, kept confidential, and protected from disclosure by the Privacy Act, as applicable. Occasionally, records obtained as evidence during the course of an investigation may contain more PII than is actually needed for the investigation, but the evidence must be preserved in the format in which it is obtained. OIG follows applicable PII safeguards. In addition, the OIG-IMS system is a secure, limited access system designed to protect ALL investigative information and records included in the system (not just PII). All OIG personnel with access to OIG-IMS are trained in proper safeguarding of PII and other investigative material, and have been cleared and trained in proper security procedures for the OIG-IMS system. Access to the system is strictly controlled and monitored.

#### **4. Uses of the Information**

##### **a. Describe all uses of the information.**

The information is used by OIG/INV to promptly investigate an allegation. If necessary, information is disclosed to joint investigative agencies or adjudicating entities. As appropriate, information is cross-checked against secure law enforcement databases to ascertain subjects' identities and to evaluate any previous criminal history to ensure agent safety. The information may also be used to generate management reports of a statistical nature (e.g., counts of active or closed cases), which are comprised only of anonymized information (i.e., information that has been stripped of all PII).

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

OIG/INV agents and analysts use their specialized investigative training to analyze system data and establish its relevance in specific cases. Only subject-based inquiries or searches of OIG-IMS system information are performed. Analytical techniques such as non-subject-based data mining, relational analysis, pattern matching, and record scoring are not performed.

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

Publicly available information, commercial information, or information from other Federal agency databases may be recompiled into the investigative record for specific cases if relevant to the applicable allegation(s).

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

OIG-IMS is supported on a U.S. Government computer platform operated by cleared NASA-OIG government employees. Federal government employees with authorized access to the NASA-OIG platform or to OIG-IMS investigative case records undergo annual security awareness training and Privacy Act rules of conduct briefing. All NASA-OIG agreements for the maintenance and operation of their computer platform on behalf of other Federal agencies include the Privacy Act clauses prescribed by the Federal Acquisition Regulation.

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

The system's control features limit its uses to compiling, managing, and tracking individual investigative records. Access for investigative purposes is limited to those

authorized Government staff members who have a need to know in performance of their official duties. Each authorized user must first sign a user access agreement before being given a user account. The user access agreement includes Privacy Act rules of conduct restricting authorized users to a clearly defined domain of permissible and prohibited uses.

## **5. Retention**

### **a. How long is information retained?**

Paper records related to allegations for which no investigative case was opened are destroyed five years after their creation in accordance with records disposition schedule A-29-001-10a. All other investigative case records that have been closed are maintained for an additional 10 years before their destruction in accordance with records disposition schedule A-29-001-10b.

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

OIG-IMS records are retained as long as may be required during the investigation and any related administrative, audit, judicial, or other operational purpose. Privacy risks are low although investigative files, including the PII contained therein, are sometimes extracted from the OIG-IMS system and shared as necessary with other federal, state, and local agencies or offices. Any personal information disclosed to another federal, state, or local agency or office in the furtherance of an investigation, prosecution or other follow-on action is accompanied by notification that it is to be used for official purposes only, kept confidential, and protected from disclosure as law enforcement sensitive information and Privacy Act material, as applicable. OIG follows law enforcement record and applicable PII safeguards. In addition, the OIG-IMS system is a secure, limited access system designed to protect ALL investigative information and records included in the system (not just PII). All personnel with access to OIG-IMS are trained in proper safeguarding of PII and all investigative material, and have been cleared and trained in proper security procedures for the OIG-IMS system. Access to the system is strictly controlled and monitored.

## **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?**

ROIs are routinely shared with the DOS Bureaus of: Human Resources, for consideration of disciplinary action; Resource Management, for collection of monies owed to the Government; and Diplomatic Security, for consideration of employee suitability. Information also may be shared with affected Department of State managers to the extent the sharing does not jeopardize the integrity of the investigation, unduly infringe on privacy rights of the accused, or jeopardize the identity of anonymous sources.

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

Information is only shared in the form of a paper ROI clearly marked “Investigative Data – Official Use Only,” that further requires a signed change of custody receipt. The minimum amount of PII is included in ROIs, which also require a signed change of custody receipt. Once returned to OIG-INV, these paper versions are promptly destroyed. Computer-readable records in OIG-IMS are not shared outside the offices of OIG.

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

The risks associated with sharing privacy information internally and disclosures of privacy information are generally associated with personnel. Intentional and unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. However, internal sharing of OIG-IMS investigative information is strictly limited to authorized users with a need to know, all of whom are cleared government employees or contractors with work-related responsibilities specific to the access and use of the information. No other internal disclosures of the information within the Department of State are made.

## **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?**

If there is sufficient evidence of criminal misconduct, investigative case records may be shared with the Department of Justice and host country, state, or local authorities under conditions of disclosure permissible under the Privacy Act or a published routine use under the system of records identified in Section 8 (below). Investigative case records of evidence of non-criminal matters may also be disclosed to the Department of State’s Director General of the Foreign Service and Director of Human Resources under the same authorities.

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

Reports of Investigation (ROIs) are only shared externally in the form of a paper record clearly marked “Investigative Data – Official Use Only.” The minimum amount of PII data is included in these ROIs, which also require a signed change of custody receipt. Electronic records in OIG-IMS are not shared outside the offices of OIG.

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

The risks to privacy from external sharing and disclosure are minimal. OIG/INV conducts investigations according to the Quality Standards for Investigations, issued by the Council of Inspectors General on Integrity and Efficiency. Adhering to these guidelines mitigates the risk of improper disclosure by ensuring system information is properly handled and protected. Any information shared with external entities is limited to disclosures permissible under the Privacy Act and bounded by the Department of State system of records notice STATE-53 routine uses.

## **8. Notice**

The system:

- contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records:

State-53, Office of Inspector General Investigation Management System.

- does NOT contain information covered by the Privacy Act.

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

Notice is provided through the publication of State-53, Office of Inspector General Investigation Management System. Also, information about subjects, witnesses, and third parties may be collected without their knowledge during the course of an investigation to ensure investigative accuracy. Individuals voluntarily report allegations to the OIG Hotline. DOS, BBG, and IBWC – U.S. section employees (including current employees, Locally Employed staff, and contract employees) are automatically granted confidentiality on any complaints made to OIG in accordance with Section 7 of the Inspector General Act and 1 FAM 053.2-5.g. Information may also be requested directly from a subject, witness, or third party during an investigative interview, subject to applicable warnings of the legal consequences of speaking or maintaining silence.

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

Individuals that report an allegation to the hotline may choose to remain anonymous. Witnesses, subjects, and third parties who are not DOS, BBG, or IBWC – U.S. section employees may decline to provide information. This may limit the ability for OIG/INV to conduct a complete investigation into the matter and may result in the investigation's closure due to insufficient information. However; as provided in 1 FAM 053.2-5.j, DOS, BBG, and IBWC – U.S. section employees generally must provide OIG with any requested information unless an employee-subject is liable for criminal prosecution and chooses to invoke his/her Constitutional Fifth Amendment right against self-incrimination.

**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?**

Individuals do not have the right to consent to or specify the uses of the investigative information that may be compiled because an investigation may relate to a possible violation of laws, regulations, codes of conduct, or ethics.

**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.**

Notice is provided through the publication of System of Records Notice (SORN) State-53, Office of Inspector General Investigation Management System. The risks to privacy from individuals being unaware of collection are minimal. Any maintenance of records with PII presents some minimal risk of inadvertent unauthorized access; however, all PII maintained in or shared from the OIG-IMS is done under the added protections of OIG's investigative process and protections that are designed to prevent unauthorized access to ALL investigative information (all "law enforcement sensitive" information, not just PII).

## 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 record notification, record access, and record contesting are published in the Privacy Act system of records notice specified in Section 8 (above) and 22 C.F.R. § 171. Individuals who have cause to believe that this system might have records pertaining to them and have inquiries about those records can write to the System Manager at the address provided in the SORN. At a minimum, the individual must include his or her: name; date and place of birth; current mailing address and zip code; signature; and other information helpful in identifying the record.

Individuals who wish to gain access to records pertaining to themselves can direct those requests, in writing, to the System Manager. The individual must specify the records being requested and must include, at a minimum, his or her name; date and place of birth; current mailing address and zip code; and signature, duly notarized or submitted under penalty of perjury (See 22 CFR part 171; 28 U.S.C. 1746). A determination as to exemption(s) is made at the time a request for access or amendment is received.

Individuals who wish to contest information in the system pertaining to themselves can write to the System Manager. The request must clearly and concisely state what information is being contested, the reason for contesting it, and the proposed amendment to the information.

Pursuant to 5 U.S.C. 552a(j)(2), the records contained within this law enforcement system of records are exempted from any part of the Privacy Act except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10) and (11), and (i).

Pursuant to 5 U.S.C. 552a (k)(1), (k)(2) and (k)(5), the records in this system are exempted from the following provisions of the Privacy Act: subsections (c)(3), (d), (e)(1), (e)(4)(G), (H) and (I) and (f). See rules published in the Federal Register, 22 CFR part 171.

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

To the extent information in OIG-IMS may be Privacy Act-covered, the notification mechanisms offered to individuals are reasonable and adequate in relation to the system's stated purposes and uses and its applicable legal requirements. Therefore, this category of privacy risk is appropriately mitigated in OIG-IMS.

## 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?**

Access to OIG-IMS is limited to authorized Department of State OIG/INV staff having an official need to access OIG-IMS in the performance of their official duties. All users maintain at least a SECRET security clearance in order to gain access. Each authorized user must first sign a user access agreement before being given a user account and being issued credentials. The user access agreement includes rules of behavior. All

federal government employees with authorized access to the NASA-OIG platform or to OIG-IMS undergo annual security awareness training and Privacy Act rules of conduct briefing. Access to OIG-IMS requires a two-factor authentication process that includes use of a one-time password crypto-token that is not part of either the investigator's desktop or the NASA-OIG computer platform that OIG-IMS resides on. The level of access for each user restricts the data that may be seen and the degree to which data may be modified. Activity by authorized users is monitored, logged, and audited. When records have reached their retention ceiling they are immediately retired or destroyed in accordance with National Archive and Records Administration records disposition schedules.

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

All users are required to undergo computer security and Privacy Act awareness training prior to being given access to OIG-IMS and must complete annual refresher training 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.**

The administrative, personnel, and technical controls described above are above and beyond typical PII protections due to the need to protect ALL information in the system as law enforcement sensitive information. Therefore privacy risk related to access is considered negligible.

## **11. Technologies**

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

No technologies are used in OIG-IMS that commonly elevate privacy risk.

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

No privacy risk exists for the use of non-standard technologies.

## **12. Security**

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

The NASA-OIG computer platform upon which OIG-IMS resides is certified and accredited for operation by NASA-OIG management and technical security personnel in accordance with the Federal Information Security Management Act (FISMA) and National Institute for Standards and Technology (NIST) standards and guidance. The current authorization to operate (ATO) was signed in August 2013, and is valid until August 6, 2016.