US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/17/2016

OPDIV:

OIG

Name:

Inspector General Support System (IGSS)

PIA Unique Identifier:

P-5300201-808702

The subject of this PIA is which of the following?

General Support System (GSS)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The Infrastructure General Support System (IGSS) provides the computing and communications infrastructure for OIG offices nationwide. It supports all OIG direct mission and administrative activities performed by the OIG under the authority of the Inspector General Act of 1978, 5 U.S.C. App. 3. It supports all of the other systems at OIG.

Describe the type of information the system will collect, maintain (store), or share.

The Infrastructure General Support System (IGSS) is not an information system in itself. It provides the computing and communications foundation for and integrates with OIG's information systems. In that capacity, it provides the first level of identification and authentication of OIG staff authorized access to OIG systems and their information. To accomplish this function, it maintains basic identity and organizational assignment information on OIG staff extracted from the Department's Enterprise Human Resource and Payroll (EHRP) System. This information may include SSN, Full Name, Driver's License Number, E-mail address, Phone numbers, Certificates, Education Records, Taxpayer ID, DOB, Mailing address, Financial Account Info, Employment status.

The Information maintained by the Corporate Mission Support System assures the OIG that only OIG staff are authenticated and provided access to OIG's computing and communications infrastructure. The system stores user credentials, audit logs for IT assets that comprise the OIG infrastructure, employee information, information on individuals who are the subject of an OIG investigation and other information collected in furtherance of the OIG law enforcement function. In addition to the information already listed, this information may include Taxpayer ID, Photographic identifiers, Vehicle Identifiers, Medical Records Number.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The IGSS system provides core and critical information technology support and services to a number of hosted applications and databases. The IGSS system is a nationwide network facilitating the data processing needs of the OIG authorized users. The System provides the hardware, software, program code and business logic to support the operation and management of OIG technology services. In addition, it provides primary security services and data security mechanisms in support of OIG applications. IGSS includes network storage.

The system contains the IT infrastructure that supports the majority of the OIG systems covered by their own Privacy Impact Assessments. The IGSS system contains assets supporting the Office of Investigations law enforcement activities, as well. This element of the IGSS system collects information on individuals who are subjects of investigations as well as ancillary information related to that investigation.

The system supports operations by providing the backbone for user management and authentication. The user credentials support this function. Audit logs are collected and maintained to enable enterprise risk management functions.

The information is maintained on a centrally managed OIG computer system.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number

Date of Birth

Name

Photographic Identifiers

Driver's License Number

Vehicle Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Financial Accounts Info

Certificates

Education Records

Employment Status

Taxpayer ID

User credentials (username/password)

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

Two primary purposes: Law enforcement activities as described in the Inspector General Act of 1978 and day-to-day administrative functions that support OIG operations

Describe the secondary uses for which the PII will be used.

None

Describe the function of the SSN.

SSN is used to unambiguously identify individuals for law enforcement purposes. It may also be used to identify employees in extracts from the EHRP system.

Cite the legal authority to use the SSN.

Inspector General Act of 1978, 5 U.S.C. App. 3

Identify legal authorities governing information use and disclosure specific to the system and program.

The legal authority for the collection is covered by Inspector General Act of 1978, 5 U.S.C. App. 3. System of Records Notice (SORN) 09-90-003 (Criminal Investigative Files of the IG) describes the uses and disclosures permitted for the investigative activities supported by the information in IGSS.

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-90-0076 Administrative Files

09-90-0003 Criminal and Investigative Files of the IG

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Other Federal Entities

Non-Governmental Sources

Public

Commercial Data Broker

Identify the OMB information collection approval number and expiration date

N/A

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Other Federal Agencies

Law enforcement activities

State or Local Agencies

Law enforcement activities

Describe any agreements in place that authorizes the information sharing or disclosure.

All information sharing is authorized under the routine uses described in the System of Records Notices or by statute.

Describe the procedures for accounting for disclosures.

Disclosures are accounted for by referring to system audit logs and by emails and other communications requesting disclosures in accordance with the routine uses described in the SORN(s).

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Individuals who are the subject of law enforcement activities are not provided notice. Employees considered to have given permission by accepting employment.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

There is no opt-out; systems must use the unique employee identified to authenticate a user to the system and to enable non-repudiation. Law enforcement activities are exempt from the opt-out requirement.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

Individuals who are the subject of law enforcement activities are not provided notice. Employees are not provided notice as opting out would preclude their accessing OIG network resources.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

Complaints are sent to system administrators or the Freedom of Information Act officer and triaged by the appropriate point of contact. Escalation for investigations is handled on a case-by-case basis.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

PII reviews are included in the annual security and privacy controls assessments. This incorporates the NIST 800-53r4 Appendix J Privacy Controls and provides an opportunity to assess the need for all of the PII in the system. Should PII elements be deemed unnecessary the appropriate steps would be taken in conjunction with the system administrator to remove those elements.

Records are maintained in a restricted area and accessed only by Department personnel. Access within OIG is strictly limited to authorized staff members. All employees are given instructions on the sensitivity of such files and the restrictions on disclosure. Access within HHS is strictly limited to employees on a need-to-know basis. All main frame computer files and printed listings are safeguarded in accordance with the provisions of the National Institute of Standards and Technology Federal Information Processing Standards 41 and 31, and the HHS Information Resources Management Manual, Part 6, "ADP Systems Security."

User credentials are unique and provide a mechanism through which all edits, modifications or deletions of data, including PII, in the system can be tracked. Audit logs are used to identify which users log in and which commands are executed.

Updates to the information in the system are directed to the system administrator, who will check the system for files requiring changes to maintain data accuracy and relevancy. The system is backed up to a remote data center and continuity of operations and disaster recovery plans are tested annually to ensure that they are effective in preserving integrity and availability of the data.

Identify who will have access to the PII in the system and the reason why they require access.

Administrators:

Require access to data in the system to make corrections, additions, and to ensure proper system functioning.

Developers:

Access data on an as-needed basis (need-to-know and minimum necessary) to execute their work tasks.

Contractors:

Direct contractors supporting system administration or system development.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Access requests are reviewed by system administrators and system owners and granted only to those with a bona fide need to access the system and interact with the data. Access is strictly limited and least privilege is in effect.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Least privilege and user account access levels.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

OpDiv and Department mandated security and privacy training, required on an annual basis.

Describe training system users receive (above and beyond general security and privacy awareness training).

Role-based training for those with elevated privileges and/or a cybersecurity related role is under development.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

OIG DAA-0468-2013-0013 - Destroy 15 years after cutoff (the end of the fiscal year in which the case was closed)

Employee Files are covered by General Records Schedule 1. They are transferred to the National Personnel Records Center within 30 days of employee separation.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Access is restricted by physical and computer-based access controls. Access is strictly limited to authorized OIG staff members based on role-based security features that limit access to system administrators, designated administrative personnel, and senior management officials. All computer files and printed listings are safeguarded using two factor authentication, encryption at rest, and access by least-privilege by employees with a demonstrated need to know in support of a business need. All information system assets are maintained in accordance with applicable federal guidelines and standards, including but not limited to access control by physical security personnel, badging requirements, lock and key, electronic locks, and other safeguards as deemed appropriate.