US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/07/2016

OPDIV:

OIG

Name:

Office Of Investigations General Support System (OIGSS)

PIA Unique Identifier:

P-3091307-605341

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.

Office of Investigations General Support System (OIGSS) is a collection of systems that provide law enforcement investigators and intelligence analysts with tools necessary to investigate fraud, waste and abuse by analyzing vast amounts of electronic data obtained pursuant to criminal, civil, and administrative investigations. The system consolidates the various elements of an investigation to provide investigators and analysts a full picture of the elements of a case. OIGSS is made up of several sub-systems. The functions of each are further described herein.

Clearwell - Gives forensics investigators and agents the power to streamline case analysis.

OIG Evidence Tracker - Browser-based barcode tracking system that enables agents to electronically scan and barcode any piece of evidence or property.

Digital Investigations Branch Unit (DIBU) VLAN - infrastructure to support OI activities.

Support Systems/Applications - Support system and applications are investigative tools that support law enforcement activities.

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

OIGSS collects large datasets of email, documents and other forms of digital evidence used in support of OIG investigations.
Information includes:

Subpoenas and related legal documents

Telephone records

Case notes

Case files
Complaint information

OIGSS user name and password
SSN

Name

Driver's License Number

Mother's Maiden Name

E-mail address

Phone numbers

Medical notes

Certificates (education, licensing)

Education Records

Military Status

Foreign Activities

Taxpayer ID

Date of birth

Photographic identifiers

Biometric Identifiers

Vehicle Identifiers

Mailing address

Medical Records Number

Financial Account Info

Legal Documents

Device Identifiers

Passport Number

Employment status

Purchase History

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

OIGSS collects, maintains and stores information collected through OIG investigations to facilitate criminal, civil, and administrative functions of the OIG. Information is forensically collected via from electronic devices with no distinction given to the type of data collected. In addition, user names and passwords for system users are maintained by the system.

The following systems make up OIGSS:

Clearwell - Gives forensics investigators and agents the power to streamline e-discovery, rapidly perform early case analysis, “cull-down” large datasets of email and documents to much smaller, relevant datasets, and quickly identify who knew what and when.

OIG Evidence Tracker: Browser-based barcode tracking system that enables agents to electronically scan and barcode any piece of evidence or property. Every item in the tracking system is identified by a unique bar code, allowing agents and managers to track location, prior movement, who has handled it, when and why. All information is stored in a database, which can be accessed online and used to account for and maintain items, compile and print reports, and perform complete system audits.

Digital Investigations Branch Unit (DIBU) VLAN: The DIBU VLAN is a private network used by the Office of Investigations to securely share data between DIBU offices located throughout the United States.

Support Systems/Applications: Support system and applications are investigative tools that support law enforcement activities.

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

Biometric Identifiers

Mother's Maiden Name

Vehicle Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Financial Accounts Info

Certificates

Legal Documents

Education Records

Device Identifiers

Military Status

Employment Status

Foreign Activities

Passport Number

Taxpayer ID

Purchase History

Investigative information which may contain personal information captured during investigations undertaken by OIG

User credentials and passwords

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?

1,000,000 or more

For what primary purpose is the PII used?

Any PII collected by the system is used in furtherance of the OIG mission to prevent fraud, waste and abused in HHS programs. This includes use in civil, criminal and administrative/enforcement actions taken as a result of an OIG audit or investigation.

Information from this system may be disclosed to:
(1) the Department of Justice in connection with requests for legal advice and in connection with actual or potential criminal prosecutions or civil litigation pertaining to the Office of Inspector General, and (2) a Federal or State grand jury, a Federal or State court, administrative tribunal, opposing counsel, or witnesses in the course of civil or criminal proceedings pertaining to the Office of Inspector General

Where federal agencies having the power to subpoena other federal agencies' records, such as the Internal Revenue Service, issue a subpoena to the Department for records in this system, the Department will make such records available.

Information from this system may be disclosed to the Department of Justice, to a judicial or administrative tribunal, opposing counsel, and witnesses, in the course of proceedings involving HHS, an HHS employee (where the matter pertains to the employee's official duties), or the United States, or any agency thereof where the litigation is likely to affect HHS, or HHS is a party or has an interest in the litigation and the use of the information is relevant and necessary to the litigation.

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

Information from this system may be disclosed to any other federal agency or any foreign, state, or local government agency responsible for enforcing, investigating, or prosecuting violations of administrative, civil, or criminal law or regulation where that information is relevant to an enforcement proceeding, investigation, or prosecution within the agency's jurisdiction under terms of the warrant.

Describe the function of the SSN.

Collected in conjunction with other PII, but not used as primary case file identifier. Used mainly as point of reference for understanding/accessing files generated by subject(s) of investigation.

Cite the legal authority to use the SSN.

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

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

OIG’s mission authorized by the Inspector General Act of 1978, 5 U.S.C. App. 3, as amended.

Pursuant to subsection (j)(2) of the Privacy Act, 5 U.S.C. 552a(j)(2), the Secretary has exempted the criminal investigative files of this system from the access, amendment, correction, and notification provisions of the Act, 5 U.S.C. 552a(c)(3), (d)(1)-(4), (e)(3), and (e)(4)(G) and (h).

The civil and administrative investigative files are exempted from certain provisions of the Act under 5 U.S.C. 552a(k)(2). Pursuant to 45 CFR 5b.11(b)(2)(ii)(D), the files are exempt from the following subsections of the Act: (c)(3), (d) (1)-(4), and (e)(4) (G) and (H).

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.

09-90-0100 Civil and Administrative Investigative Files of the IG

09-90-0003 Criminal Investigative Files of the Inspector General

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Foreign

Other Federal Entities

Non-Governmental Sources

Public

Commercial Data Broker

Media/Internet

Private Sector

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.

Within HHS

Enforcing, investigating, or prosecuting violations of administrative, civil, or criminal law or regulation where that information is relevant to an enforcement proceeding, investigation, or prosecution within the agency's jurisdiction under terms of the warrant.

Other Federal Agencies

Enforcing, investigating, or prosecuting violations of administrative, civil, or criminal law or regulation where that information is relevant to an enforcement proceeding, investigation, or prosecution within the agency's jurisdiction under terms of the warrant.

State or Local Agencies

Enforcing, investigating, or prosecuting violations of administrative, civil, or criminal law or regulation where that information is relevant to an enforcement proceeding, investigation, or prosecution within the agency's jurisdiction under terms of the warrant.

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

Information is provided to the Treasury Do Not Pay system (MOU)

Describe the procedures for accounting for disclosures.

Release of documentation outside of investigative activity is documented within investigative files.

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

There is no process in place to notify individuals that their PII will be collected because pursuant to subsection (j)(2) of the Privacy Act, 5 U.S.C. 552a(j)(2), the Secretary has exempted the criminal investigative files of this system from the access, amendment, correction, and notification provisions of the Act, 5 U.S.C. 552a(c)(3), (d)(1)-(4), (e)(3), and (e)(4)(G) and (h).

The civil and administrative investigative files are exempted from certain provisions of the Act under 5 U.S.C. 552a(k)(2). Pursuant to 45 CFR 5b.11(b)(2)(ii)(D), the files are exempt from the following subsections of the Act: (c)(3), (d) (1)-(4), and (e)(4) (G) and (H).

Is the submission of PII by individuals voluntary or mandatory?

Mandatory

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 option to object to information collection because this information is collected in support of enforcements, investigations and prosecutions. There is no option to opt-out of providing a unique user name to access the system - the user credential allows for authentication and non-repudiation of system activities logged by a unique user.

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

No consent is needed from individuals. The system is used by law enforcement for investigative and intelligence purposes and their request for creation of an account is considered consent to use their account credentials for that purpose. Further, the unique user name is required for system auditing purposes and the OIG transition to full PIV-enabled single-sign on will minimize the opportunity for the loss/leakage of user name PII.

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.

There is no option to object to information collection because this information is collected in support of enforcements, investigations and prosecutions. If system users believe that their information (user credentials/password) have been inappropriately obtained, used or disclosed they may report the issue to the system administrator who will initiate the appropriate review and escalate for investigation as needed.

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

As the files contain investigative information for criminal , civil and administrative investigations, and Pursuant to subsection (j)(2) of the Privacy Act, 5 U.S.C. 552a(j)(2), the Secretary has exempted the criminal investigative files of this system from the access, amendment, correction, and notification provisions of the Act, 5 U.S.C. 552a(c)(3), (d)(1)-(4), (e)(3), and (e)(4)(G) and (h); and

The civil and administrative investigative files are exempted from certain provisions of the Act under 5 U.S.C. 552a(k)(2). Pursuant to 45 CFR 5b.11(b)(2)(ii)(D), the files are exempt from the following subsections of the Act: (c)(3), (d) (1)-(4), and (e)(4) (G) and (H).

On a regular basis authorized staff may update information as additional/corrected information becomes available during an investigations. Absent this and management oversight, and in conjunction with the exemptions, there is no process as outlined.

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

Users:

As authorized law enforcement personnel creating investigative case files

Administrators:

Maintenance of accounts and administration of data

Others:

Other law enforcement investigators personnel whom have the appropriate law enforcement credentials and possess a bona fide need for access.

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

Access to PII requires possession of valid law enforcement credentials and demonstration of a bona fide need to access an OIGSS file. After review of the above an account will be created granted the necessary permissions based on the need.

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.

The system security plan outlines the access requirements and through the Administrative Tracking Application (ATA), an internal hierarchy is implemented which limits access to OIGSS systems to law enforcement personnel with appropriate need to know.

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.

Annual Departmental and OIG training to ensure staff is aware their responsibilities for protecting the information being collected and maintained. Additionally, refresher training on a regular basis for current staff and initially at new employee training.

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

Additional role-based training is planned for OIG personnel who routinely access sensitive information.

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.

Unique OIG records and disposition is documented in the following NARA approved record schedules:

OIG DAA-0468-2013-0013 - Destroy 15 years after cutoff (end of fiscal year after investigation is closed)

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

PII is secured via the following sets of controls:
Administrative controls: Access is provided based on a demonstrated need to know, appropriate job responsibilities, and proof of law enforcement status.

Technical controls: User Identification, Passwords, Firewalls, Virtual Private Network (VPN) solutions, Intrusion Detection Systems (IDS), Common Access Cards (CAC), Smart Cards, Biometrics, Public Key Infrastructure (PKI)

Physical Controls: Guards, Identification Badges, Key Cards, Closed Circuit TV (CCTV) and alarm systems.