Office of the Inspector General

Privacy Impact Assessment
for the
Inspector General Network for Telecommunication and Exchange (IGNITE) System

Issued by:
William Blier, OIG Senior Component Official for Privacy

Approved by: Erika Brown Lee, Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: [1/18/2017]

(May 2015 DOJ PIA Form)

EXECUTIVE SUMMARY

The United States Department of Justice (DOJ or Department), Office of the Inspector General (OIG), employs a general support system entitled the Inspector General Network for Information and Technology Exchange (IGNITE) System. The primary functions of this system include, but are not limited to, e-mail, word processing, spreadsheet, presentation, project management, file and printer sharing, and access and storage to databases and minor applications utilized for the OIG to effectively carry out its mission to detect and deter waste, fraud, abuse, and misconduct in DOJ programs and personnel. Specifically, the IGNITE System boundary contains the Investigations Database Management System (IDMS), which manages information relating to OIG's authorized investigations of alleged criminal, civil, or administrative violations relating to DOJ employees, contractors and other individuals and entities associated with the Department, and the TeamMate System, which is an audit management software system that tracks the electronic work papers and reports associated with an OIG Audit.

In order to carry out these OIG functions, the IGNITE System may need to store, process, and transmit personally identifiable information (PII). Because of the PII collected, used, retained, and disseminated within the IGNITE System, this Privacy Impact Assessment (PIA) was prepared and published.

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) The purpose that the records and/or system are designed to serve:

The OIG is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in DOJ programs and personnel, and to promote economy and efficiency in those programs. The OIG investigates alleged violations of criminal and civil laws by DOJ employees and also audits and inspects DOJ programs.

The IGNITE System's primary functions include e-mail, word processing, file and printer sharing, and access and storage to databases and minor applications that support OIG audits, inspections, authorized investigations, reviews, and administrative functions. The system is connected to the Internet through a trusted path using the Justice Consolidated Network (JCN). The general support system is accessed by all OIG employees and contractors. However, access to the databases, applications, and word processing documents are limited to only the employees who have a need-to-know to accomplish their job functions, as detailed below.

(b) The way the system operates to achieve the purpose(s):

The IGNITE System operates to achieve this purpose by providing four main services: email, collaboration portals/repositories, file and print services, and minor databases and web applications. The IGNITE System is an Active Directory domain that is a group of server computers that share a common user account database. The user is then able to log in to the domain through an access point to access resources that are shared on the database. User access points to the database include server computers, printers, and workstations, which are connected to the IGNITE System network. Commercially available software is used for the operating systems and software applications. General support functions are provided through these standard, commercially available software applications. OIG personnel use the IGNITE System to access the Internet for research purposes and to share information with external organizations, where appropriate.

(c) The type of information collected, maintained, used, or disseminated by the system:

The type of information collected, maintained, used, or disseminated by the system includes: identifying numbers, personal data, work–related data, and distinguishing features of DOJ employees, grantors, subjects of investigations, whistleblowers, witnesses, DOJ prisoners, and other information necessary to carry out OIG audits, authorized investigations, reviews, and inspections. The IGNITE System also contains shared drives and SharePoint sites that contain identifying numbers, personal data, work-related data, and distinguishing features. This includes data pertaining to individuals' assets and criminal history. Finally, the system maintains logs of DOJ user activity, and maintains OIG administrative files and records, such as correspondence received by the OIG from the general public and logs of OIG Freedom of Information/Privacy Act requests.[1]

(d) Who has access to information in the system?

Only DOJ employees and authorized contractors may have system user accounts. OIG Active Directories will be used for identification and authentication of users. Within the IGNITE System, access to minor applications and databases is given only to employees whose job-related duties require their access. For example, access to the Investigations Data Management System (IDMS)—a database management system used to track and monitor complaints, referrals, and authorized investigations—is given only to employees of the OIG's Investigations Division and other specifically authorized personnel. Access to the TeamMate system—a

[1] The IGNITE System also contains PII that relates to internal government operations, such as employee training and credential tracking databases. While these operations may be addressed in this PIA through their relation to the larger IGNITE System, this PIA focuses primarily on the IGNITE System's collection and maintenance of PII about members of the general public. *See* Office of Management and Budget M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 26, 2003) (stating that a PIA is not required for a government-run websites, IT systems or collections of information to the extent that they do not collect or maintain information in identifiable form about members of the general public (this includes government personnel and government contractors and consultants)).

proprietary database that tracks the electronic work papers and reports associated with an Audit—is given only to employees working on OIG audits.

(e) How information in the system is retrieved by the user:

Information in the system is accessed using workstation/laptop client software, via a web browser, mobile device, or shared files. DOJ user directory information can be retrieved by DOJ users by name or other user identifier. Privileged users can retrieve audit log information by a DOJ user's name or other identifier. Depending on the application used, some information can be retrieved by text searches.

(f) How information is transmitted to and from the system:

Information is transmitted to and from the IGNITE System through the connections noted in Section 1(g) below. These interconnections are all within DOJ boundaries and utilize firewalls and other applicable security measures. All email traffic that traverses to DOJ users will continue to route through the existing Secure Email Gateway (SEG), which provides anti-spam and anti-malware capabilities. All email traffic exiting or entering the DOJ network is inspected by the DOJ Trusted Internet Connection (TIC), which is monitored by the Justice Security Operations Center. The TIC also monitors the information system for any external unencrypted emails sent externally that contains PII, and blocks the email if it does not meet DOJ encryption policy. Remote access to the system will be accomplished using DOJ Connect with secure sockets layer encryption.

(g) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects):

There are no interconnections with systems outside of the Department. All interconnections are within DOJ information system boundaries, including the following:

- Justice Unified Telecommunications Network (JUTNet) (for wide-area networking connectivity).
- Trusted Internet Connection at Justice Data Centers (for internet connectivity, including email routing to and from Internet email addresses).
- DOJ Connect (for remote access).
- Federal Bureau of Prisons (BOP) Databases (including SENTRY and Trueview Databases).
- OIG Active Directory (for identification and authentication of users)

(h) Whether it is a general support system, major application, or other type of system:

The IGNITE System is a general support system that includes minor applications, including:

- IDMS: IDMS collects information in order for the OIG to meet its investigative and reporting responsibilities. The OIG uses IDMS to manage information relating to its authorized investigations of alleged criminal, civil, or administrative violations relating to DOJ employees, contractors and other individuals and entities associated with the Department. IDMS is a combination of a database management system (LawManager) and a document management system (i-Manage). IDMS also connects to the Reports on Investigation (ROI) tracking system, which tracks the progression of OIG Reports on Investigation written by OIG agents and submitted thru their local field and area offices. IDMS collects, maintains, and uses identifying numbers, personal data, work-related data, and distinguishing features, and may also include tip and complaint information submitted voluntarily by the public through the OIG Hotline.[2] Access is given to employees of the OIG's Investigations Division, which includes Special Agents, Investigative Specialists, and support staff. Information in the system is retrieved by users either directly from the individual about whom the information pertains, government sources, and non-government sources, such as the media.

- The TeamMate System: TeamMate is an audit management software system that tracks the electronic work papers and reports associated with an OIG Audit. The system collects, maintains, and uses identifying numbers, personal data, work –related data, and distinguishing features. Access is given to auditors and program analysts who perform OIG audits. Information in the system is retrieved by users either directly from the individual about whom the information pertains, government sources, and non-government sources, such as the media.

- General Administrative Support Applications: The IGNITE System also contains administrative support applications for the purpose of assisting OIG employees in successfully implementing OIG functions. For instance, the OIG utilizes the FOIAExpress software system to manage Freedom of Information Act (FOIA) and Privacy Act requests. This application manages the entire request to response process, including correspondence and document management. Information in FOIAExpress is searchable by a requester's name or assigned number. The information entered into the system includes a requester's name, address, and email address. Requesters are required to submit a Certificate of Identity form, which may include his/her social security number and date of birth. This form is then scanned into the FOIAExpress database, where it is searchable by name or assigned request number.

[2] *See* https://oig.justice.gov/hotline/.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers							
Social Security	X	Alien Registration	X	Financial account	X		
Taxpayer ID	X	Driver's license	X	Financial transaction	X		
Employee ID	X	Passport	X	Patient ID	X		
File/case ID	X	Credit card	X				
Other identifying numbers (specify):							

General personal data							
Name	X	Date of birth	X	Religion	X		
Maiden name	X	Place of birth	X	Financial info	X		
Alias	X	Home address	X	Medical information	X		
Gender	X	Telephone number	X	Military service	X		
Age	X	Email address	X	Physical characteristics	X		
Race/ethnicity	X	Education	X	Mother's maiden name	X		
Other general personal data (specify): For OIG administrative matters, primary and secondary emergency contact information, including names, addresses and phone numbers. For OIG investigative matters: a general description of subjects' suspected criminal activities and associates; Data pertaining to individuals' assets including: where the asset was seized (physical address), agent who conducted seizure, and case numbers associated with seizure event; and Criminal History data. Additional PII in the system includes: Information about DOJ employees such as name, job title, and work contact info; Information from BOP's SENTRY Database including Inmates' Security Level and Date Classified; Country of Citizenship; Sentencing and Release Dates; Offense Category; Criminal History Points; Designated Facility; Public Safety Factor; Management Variable; Information from Consolidated Debt Collection System (CDCS); Hiring data from the National Finance Center and from agency-level Human Resource Managers.							

Work-related data							
Occupation	X	Telephone number	X	Salary	X		
Job title	X	Email address	X	Work history	X		
Work address	X	Business associates	X				

Work-related data
Other work-related data (specify): Information related to security clearance risk level; Training Agendas containing employee name and position; employee training travel forms containing pay grade information.

Distinguishing features/Biometrics					
Fingerprints	X	Photos	X	DNA profiles	X
Palm prints	X	Scars, marks, tattoos	X	Retina/iris scans	X
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify):					

System admin/audit data					
User ID		Date/time of access	X	ID files accessed	
IP address		Queries run	X	Contents of files	

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person	X	Hard copy: mail/fax		Online	X
Telephone	X	Email	X		
Other (specify): Computer Forensic data (from forensic evidence taken by the OIG Investigations Division); data retrieved through the Asset Forfeiture Management Staff Portal; information submitted directly from individuals via the OIG Hotline.					

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal	X	Foreign	X		
Other (specify): National Finance Center, Congress.					

Non-government sources					
Members of the public	X	Public media, internet	X	Private sector	X
Commercial data brokers	X				
Other (specify):					

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Potential threats include cyber attacks that lead to identity theft of the individuals whose information was collected and the safety and security of participants in the programs under review. This includes DOJ employees and contractors, federal inmates, and debtors and grantors in DOJ databases, and other individuals who may be victims, complainants, or subjects of an authorized OIG investigation.

The data above represents data that is or may be collected during authorized OIG investigations, audits, inspections, reviews, or other administrative tasks. The data above also represents data that is or may be collected when individuals file complaints with the OIG. Social Security information is collected to uniquely identify individuals (e.g., subjects, witnesses, complainants) and for other investigative purposes such as running criminal history checks and obtaining other relevant records. Use of a social security number ensures that that the OIG can distinguish between individuals who may have the same name, date of birth, or other identifying information in common.

Another potential threat to privacy in light of the information collected is that the system will collect and/or maintain more information than is relevant and necessary to accomplish the Department's official duties. Through OIG and DOJ-wide guidance and policy, the OIG provides continuous awareness to employees on the proper handling of PII. For example, the OIG Audit Division policy discourages collecting PII from auditees, however, collection of PII is sometimes unavoidable depending on how an auditee keeps its records and the scope of the authorized audit. As a result, the OIG Audit Division has formal policies that address the proper storage and transfer of PII.

The OIG collects information only where it has specific legal authority to do so and the information is required to meet OIG's responsibilities. When feasible, the OIG collects the minimum amount of information needed to cross-check multiple data sets and identify individual records, or to document the completion of OIG work and findings. Wherever possible, the teams remove PII from the data sets prior to conducting analysis. Once the work is completed, the data is stored and managed according to the applicable records retention schedule for each IGNITE System application. For more information about records management and NARA records schedules for the OIG, see responses to question 3.4. The majority of the data collected by the OIG comes from DOJ agency databases or from individual employees. The IGNITE System itself is not the original collector of much of the information that it maintains about individuals. For example, many of the documents are received from other components within the Department of Justice in response to data calls related to OIG audits,

authorized investigations, and inspections. In addition, it may not be feasible to collect information directly from the subject of an investigation due to the fact that the subject may be unaware that he/she is a person of interest.

For information about the security controls that have been applied to the IGNITE System that assist in mitigating threats related to the collection of PII, please see the responses to questions 6.1 and 6.2, below

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities	X	For civil enforcement activities
	For intelligence activities	X	For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
X	To conduct analysis to identify previously unknown areas of note, concern, or pattern.	X	For administering human resources programs
X	For litigation		
X	Other (specify): Program evaluation, analysis, and oversight. Research into a complainant's Hotline issues for a response to the complainant		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

The IGNITE System's criminal and investigative function uses collected information for the purpose of conducting OIG authorized criminal, civil and/or administrative investigations. The application that collects PII for criminal and administrative investigations is IDMS. IDMS is a combination of a database management system (LawManager) and a document management system (i-Manage). Information in IDMS will be used in order to meet OIG's statutory responsibilities to conduct investigations relating to DOJ projects, programs, and operations. The ROI Tracking System –which tracks the progression of the ROI written by OIG agents and submitted thru their local field and area offices—is linked to IDMS using the investigation case number. The electronic version of the ROI is located in the i-Manage document management repository application. Overall, the OIG uses the information maintained in IDMS in order to conduct authorized criminal, civil, and/or administrative investigations relating to DOJ programs and operations. As explained above, the OIG collects SSNs for the purpose of verifying the identity of subjects, complainants, witnesses, and third

parties and for other investigative purposes, such as running criminal history checks and obtaining other relevant records.

The applications within the IGNITE System that collect PII for non-criminal investigative matters are the Teammate and the SharePoint Databases. The Teammate system is used by the OIG's Audit Division, the OIG's largest division made up of 200 skilled auditors, program analysts, statisticians and other operational staff. Through its multi-disciplined staff, the Audit Division conducts performance audits of Department programs and operations and oversees annual audits of over $35 billion in Department expenditures. The Division also conducts audits of external entities that receive Department funding through its various contracts and grant programs. These audits significantly assist the Department in its efforts to prevent waste, fraud and abuse, and to promote economy and efficiency in its operations. The Division's robust oversight program is primarily driven by risk-based assessments of Department operations, as well as legal mandates, congressional requests, current events, and the Department's Top Management and Performance Challenges as identified by the OIG each year. Teammate is a proprietary database that tracks the electronic work papers and reports associated with an Audit.

SharePoint and other files within IGNITE contain PII for the aforementioned purposes in addition to administrative matters. The SharePoint Portal (OIGPortal) is the OIG's internal unclassified enterprise intranet and collaboration platform, used by all OIG employees and contractors. The OIGPortal provides video training, links to DOJ websites and other online government resources, application access, and standard templates that assist employees in performing their functions according to OIG standards. Its collaboration areas house work in progress as well as final products of both administrative and mission-related tasks and projects. In addition, the platform provides electronic forms, tools, and workflows that streamline internal processes. Both static content areas and collaboration areas apply appropriate permissions and banner notices to identify and restrict access to sensitive material.

Outside of these databases, the IGNITE System also contains PII collected during OIG reviews and administrative security and human resources matters. For example, information maintained in the FOIAExpress application will enable the appropriate Divisions/Offices within OIG to administratively control and/or process requests for records.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
X	Statute	IG Act, 5 U.S.C App 3 ; Attorney General Order 1393-90
	Executive Order	
	Federal Regulation	

X	Memorandum of Understanding/Agreement	Including but not limited to, "OIG/BOP Memorandum of Understanding Covering OIG Access to BOP Truview Database"
X	Other	28 C.F.R. Part 16, Production or Disclosure of Material or Information; DOJ Order 2640.2F – Information Technology Security; DOJ Order 2740.1A – Use and Monitoring of DOJ Computers and Computer Systems; DOJ Order 0903, Information Technology (IT) Management. Various DOJ component mission authorities (including statutes, Executive Orders, and regulations)

3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

The IGNITE System stores and manages different types of records across its many business-specific applications. Overall, information is retained until it is deemed no longer necessary to support OIG investigations or reports, or its other authorized functions. Information is disposed of through deletion from the network drives, using the standard OIG records retention schedule, which varies based on the type of data and the OIG division it belongs to.

Applications that manage permanent records are governed by OIG's NARA records schedules, while applications that manage temporary records are governed by either the General Records Schedule (GRS) or a NARA records schedule. The OIG Records Manager maintains a listing of all OIG records schedules and applicable GRS items, which is annually updated and customized for each OIG Division/Office to create a detailed file plan. Each Division/Office uses the file plan to manually conduct their own records disposition in coordination with the OIG Records Manager and the IGNITE System administrators/owners. NARA records schedules for the IGNITE System's major applications include but are not limited to: Investigations Database Management System (IDMS) [N1-060-09-066]; Report of Investigations Tracking System [DAA-0060-2012-0014]; Audit Management System (TeamMate) [N1-060-09-072]; Project Proposal Database [N1-060-11-003]; and O&R Case Tracking System [N1-060-09-027].

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users

regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Potential threats include identity theft of the individuals whose information was collected and the safety and security of participants in the programs under review. The OIG restricts access to this information to only the employees who have a need to know. If information is provided by Department agencies via CDs, they are password-protected and locked in filing cabinets within OIG controlled office space. Information that is provided via e-mail is stored in files in restricted-access folders and libraries. Hard copies of documents are shredded when no longer needed. For a list and description of some of the security controls that have been put into place to safeguard against these and other risks, please see the responses to questions 6.1 and 6.2.

In addition, OIG employees receive mandatory annual computer awareness training and records management training.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X	X	X	Direct Access to Project
DOJ components	X			
Federal entities	X			
State, local, tribal gov't entities	X			
Public	X			
Private sector	X			
Foreign governments	X			
Foreign entities				
Other (specify): White House	X			

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of

the information – training, access controls, and security measures; etc.)

The system is accessible by DOJ employees and contractors only and utilizes tiered, role-based access commensurate with the user's official need to access information. The user's role and work assignments will determine their access to the applications within the IGNITE System, such as IDMS, Teammate, and the SharePoint Database. Physical access to system servers is controlled through site-specific controls and agreements. Employees complete annual training on handling sensitive information. Wherever possible, PII is removed from data sets before analysis.

Data provided to DOJ Components relates to information they already possess, or relates to an investigation for which the release is appropriate. The specific external entities with which the OIG shares information maintained in the IGNITE System depends on the nature, subject, status, and other factors unique to each circumstance. Such disclosures would be on a case-by-case basis and involve approvals at the appropriate management level such as senior Investigations Division management level, the Office of General Counsel, or the Inspector General. For instance, if an investigation involves persons employed by other Federal, State, or local agencies, information may be shared with those other agencies. If a case is referred for prosecution, information will be shared with the Federal, State, or local prosecutors and/or law enforcement agencies. Information may also be shared with Congressional Committees with jurisdiction over matters under investigation. Disclosure of any such information is done consistent with Federal law and Department policies. In addition, any information that is disclosed or shared, including reports, investigative files, correspondence, and memoranda, undergoes a privacy review to minimize the risk of unauthorized disclosure, and is disclosed consistent with Federal law and Department policies.

The OIG also has a number of technical safeguards in place to assist in mitigating risks associated with the authorized disclosure of PII in the IGNITE System. For example, the OIG requires that all PII be encrypted if it is emailed outside the Department of Justice's network. Any Social Security Numbers that are detected in an email are automatically blocked if the email is not encrypted. For additional safeguard, please see the responses to questions 6.1 and 6.2.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a System of Records Notice published in the Federal Register and discussed in Section 7.	
X	Yes, notice is provided by other means.	Specify how: See Section 5.4 below regarding OIG Hotline.
X	No, notice is not provided.	Specify why not: See Section 5.4 below regarding authorized OIG investigations.

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: See Section 5.4 below regarding OIG Hotline.
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: See Section 5.4 below regarding authorized OIG investigations.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

X	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: See Section 5.4 below regarding OIG Hotline.
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: See Section 5.4 below regarding authorized OIG investigations.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

The OIG is authorized to conduct certain criminal, civil and/or administrative investigations. Information related to these investigations, including PII, may be maintained in the IGNITE System. In certain circumstances, the subject of an authorized OIG investigation cannot be provided with direct notice and an opportunity to consent because such notice would provide the subject of an investigation with substantial information which could impede or compromise the investigation. Providing such notice to a subject of an investigation could interfere with an undercover investigation by revealing its existence, and could endanger the physical safety of confidential sources, witnesses, and investigators by revealing their identities. To the extent that content contained in such communications is protected by Federal law, including the Privacy Act, notice is provided by various DOJ Privacy Act Systems Of Records Notices (SORNs), detailed in Section 7, which apply depending on how information is retrieved. These notices and documents are published in the Federal Register, on the Department SORNs webpage,[3] and are available to the general public.

In addition, the OIG maintains a hotline by which individuals can report allegations of waste,

[3] https://www.justice.gov/opcl/doj-systems-records.

fraud and abuse, misconduct, or whistleblower reprisal relating to a DOJ employee, program, contract, or grant (OIG Hotline). Submission of any information is voluntary, and individuals who report allegations are not required to provide their identity to the OIG. However, persons who report allegations are encouraged to identify themselves to help the OIG evaluate and investigate the complaints. Confidentiality for complainants is established by Section 7(b) of the Inspector General Act of 1978, which prohibits the OIG from disclosing the identity of a DOJ employee who reports an allegation or provides information, without the employee's consent, unless the OIG determines that disclosure is unavoidable during the course of the authorized OIG investigation. The OIG also provides the public with information regarding the OIG's jurisdiction over complaints, confidentiality for complainants, and other privacy-related notices on its OIG Hotline webpage.[4]

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: November 2015 If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:
X	A security risk assessment has been conducted.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: This system is a FISMA high system, and applies all NIST 800-53 high baseline security controls. Appropriate security controls that have been identified and implemented to protect against risks identified in the security risk assessment include those listed in DOJ Security Assessment and Authorization Handbook v. 8.4, which provides the framework and direction for performing security assessments and authorizations of all DOJ IT systems.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: The system has undergone assessments, penetration tests, vulnerability scans, and is monitored by other means by the OIG Information Systems Security Officer.
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: Audit logs are maintained to help ensure compliance with tiered/role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information, including PII. Audit logs can only be accessed by authorized staff as required to ensure compliance with security requirements.
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.

[4] https://oig.justice.gov/hotline/info.htm.

X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
X	The following training is required for authorized users to access or receive information in the system:	
	X	General information security training
	X	Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

The IGNITE System implements all NIST SP 800-53, Revision 4 security controls required for high impact systems. The control families include categories to address awareness, training, access control, system boundary protection, and other controls to reduce the risk of unauthorized access and disclosure. Specifically, these controls include, but are not limited to the following:

- IGNITE utilizes tiered, role-based access commensurate with the user's official need to access information. Physical access to system servers is controlled through site-specific controls and agreements.
- IGNITE is protected by multiple firewalls, an intrusion prevention system, real-time continuous monitoring using malicious code detection and protection, encryption, and other technical controls in accordance with applicable security standards.
- All email traffic routes through the existing Secure Email Gateway, which provides antispam and anti-malware capabilities. All email traffic entering or exiting the DOJ network is additionally inspected by the DOJ Trusted Internet Connection, which is monitored by the Justice Security Operations Center.
- All users must complete annual computer security awareness training, as well as read and agree to comply with DOJ Information Technology Rules of Behavior both prior to accessing the DOJ network and annually thereafter. The IGNITE System administrators must complete additional professional training, which includes security training. In addition, all IGNITE System users must complete privacy training on handling and protecting PII.

The IGNITE System undergoes an annual assessment to review the current state of its implementation of all required controls.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created or has already been created in accordance with the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing System of Records Notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: • JUSTICE/OIG-001, Office of the Inspector General Investigative Records, 72 Fed. Reg. 36725 (July 5, 2007); • JUSTICE/OIG-004. Office of the Inspector General, Employee Training Records. 72 Fed. Reg. 68375 (Dec. 7, 1999) (as modified by 66 Fed. Reg. 8425 (Jan. 31, 2001), and 72 Fed. Reg. 3410 (Jan. 25, 2007)); • JUSTICE/OIG-005, Office of the Inspector General, Firearms Qualifications System, 72 Fed. Reg. 68376 (Dec. 7, 1999) (as modified by 66 Fed. Reg. 8425 (Jan. 31, 2001), and 72 Fed. Reg. 3410 (Jan. 25, 2007); • JUSTICE /DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, 77 Fed. Reg. 26580 (Mar. 4, 2012) • JUSTICE/DOJ-002, DOJ Computer Systems Activity & Access Records, 64 Fed. Reg. 73585 (Dec. 30, 1999) (as modified by 66 Fed. Reg. 8425 (Jan 31, 2001), and 72 Fed. Reg. 3410 (Jan. 25, 2007)); and • Other published Government-wide and DOJ System of Records Notices, depending on the nature of information in the communication or collaboration document and how the information is retrieved.
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Some records contained in the IGNITE System are retrieved by identifying information and are covered by existing SORNs. These categories of information include, but are not limited to: investigative records in the IDMS system (covered by JUSTICE/OIG-001); FOIA/Privacy Act records (covered by JUSTICE/DOJ-004); employee training records (covered by JUSTICE/OIG-004); employee firearms qualification systems records (covered by JUSTICE/OIG-005); and access logs and other audit records for individuals who access DOJ network computers or mainframe/enterprise servers, including individuals who send and receive electronic communications, access Internet sites, or access system databases, files, or applications from DOJ computers (covered by JUSTICE/DOJ-002).