U.S. Department of Commerce

Office of Inspector General (OIG)

Privacy Impact Assessment
For the
OIG General Support System

Reviewed by: Toan Pham, Bureau Privacy Officer or Designee

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.09.26 16:18:44 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Office of Inspector General

Unique Project Identifier: IT Infrastructure System (OIG0001)

Introduction: System Description

(a) a general description of the information in the system, and
(b) a description of a typical transaction conducted on the system:

The OIG General Support System (GSS) provides general operational IT services and support for the mission and activities of the OIG; network user authentication and access; e-mail service; file processing, sharing, and storage; application and database development, update, and management; print services; and overall system security (including patch and antivirus management). The OIG GSS supports all business essential and office automation applications for all OIG components.

(c) any information sharing conducted by the system

Information may be shared with the following agencies: Government Accountability Office, Office of Special Counsel, Equal Employment Opportunity Commission, National Finance Center, Agency for International Development, General Services Administration, Federal Deposit Insurance Corporation, Federal Housing Finance Agency, Federal Trade Commission, Merit Systems Protection Board, National Aeronautics and Space Administration, National Archives and Records Administration, National Science Foundation, Office of Government Ethics, Office of Personnel Management, Postal Service, Pension Benefit Guaranty Corporation, Securities and Exchange Commission, Small Business Administration, Smithsonian Institute, Social Security Administration, Veterans Administration, Office of Management and Budget, other OIGs, Federal Bureau of Investigations, and other agencies in the Department of Justice. Information may also be shared with other Federal agencies on a case-by-case basis. Additionally, on a case-by-case basis, information may be shared among the OIG offices; with Departmental offices and operating units; with state, local, and tribal government agencies; Congress; and with the public.

(d) a citation of the legal authority to collect PII and/or BII

Pursuant the Inspector General Act of 1978 (IG Act), as amended, 5 U.S.C. app. 3 § 6, OIG has the legal authority to conduct investigations and audits and conduct routine activities of a government agency that may require the collection of PII and/or BII.

(e) The Federal Information Processing Standard (FIPS) 199 security impact category for this system is moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

_X_ This is an existing information system with changes that do not create new privacy risks.

(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security[1]	x	e. Alien Registration		i. Financial Account	x
b. Taxpayer ID	x	f. Driver's License	x	j. Financial Transaction	x
c. Employee ID	x	g. Passport	x	k. Vehicle Identifier	x
d. File/Case ID	x	h. Credit Card	x	l. Employer ID Number	x
m. Other identifying numbers (specify):					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth	x	m. Religion	
b. Maiden Name	x	h. Place of Birth	x	n. Financial Information	x
c. Alias	x	i. Home Address	x	o. Medical Information	x
d. Gender	x	j. Telephone Number	x	p. Military Service	x
e. Age	x	k. Email Address	x	q. Physical Characteristics	x
f. Race/Ethnicity	x	l. Education	x	r. Mother's Maiden Name	x
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	x	d. Telephone Number	x	g. Salary	x
b. Job Title	x	e. Email Address	x	h. Work History	x
c. Work Address	x	f. Business Associates	x		
i. Other work-related data (specify):					

[1] Situations in which Social Security Numbers would be collected are: for litigation, for civil enforcement activities, for administering human resources programs, for criminal law enforcement activities, for intelligence activities supporting the intelligence activity of the Department's Office of Security, and through OIG's data loss prevention tool that quarantines unencrypted e-mails that contain PII in plaintext to prevent PII spillage.

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	x	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics(specify):					

System Administration/Audit Data (SAAD)					
a. User ID	x	c. Date/Time of Access	x	e. ID Files Accessed	x
b. IP Address	x	d. Queries Run	x	f. Contents of Files	x
g. Other system administration/audit data (specify):					

2.2 Indicate sources of the PII/BII in the system. *(Check all thatapply.)*

Directly from Individual about Whom the Information Pertains					
In Person	x	Hard Copy: Mail/Fax	x	Online	x
Telephone	x	Email	x		
Other (specify):					

Government Sources					
Within the Bureau	x	Other DOC Bureaus	x	Other Federal Agencies	x
State, Local, Tribal	x	Foreign	x		
Other (specify): X – Freedom of Information Act (FOIA) requests					

Non-government Sources					
Public Organizations	x	Public Media, Internet	x	Private Sector	x
Commercial Data Brokers					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all thatapply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	X	Building entry readers	x
Video surveillance		Electronic purchase transactions	x
Other (specify): OI transfers audio files to a secure file system CMS.			

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the system is being collected, maintained, ordisseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	x
For administrative matters	x	To promote information sharing initiatives	
For litigation	x	For criminal law enforcement activities	x
For civil enforcement activities	x	For intelligence activities (To support the intelligence activity of the Office of Security)	x
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): - OIG's data loss prevention tool quarantines unencrypted e-mails that contain PII information in plaintext to prevent PII spillage.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations,etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

PII is collected for administrative uses for all offices in OIG and would typically be in reference to items checked in Section 2.1 for IN, GPD, and WRD. PII/BII also may be collected and disseminated in support of civil or criminal law enforcement activities and litigation. The PII that is collected for administrative uses for all offices in OIG is necessary to help support the administrative activities of OIG so that OIG can accomplish its mission and support the Department. In addition, when civil or criminal law enforcement activities and litigation are in process, PII/BII may be collected and needed to support the research and investigation that occurs with those activities.

The PII/BII identified in Section 2.1 is in reference to federal employees/contractors in most instances and on a case by case basis to members of the public.

Section 6: Information Sharing

6.1 Indicate with whom the bureau intends to share the PII/BII in the system and how the PII/BII will be shared.

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	x		
DOC bureaus	x		
Federal agencies	x		
State, local, tribal gov't agencies	x		
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify): Congress	x		

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. It is transmitted via secure email, secure file transfer to secure OIG applications.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	x
Contractors	x		
Other(specify): Government employees and government contractors who have an appropriate clearance and need to know for their work purposes can access OIG specific applications such as OI, HR, Data Analytics, resident within the GSS system(s) authorized to process PII and/or BII.			

Section 7: Notice and Consent

7.1 Indicate whether individuals/employees will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all thatapply.)*

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: On the publicly accessible OIG website (http://www.oig.doc.gov), there is a link to the Privacy Policy at the bottom of the page. In addition, on the Hotline & Whistleblower Protection section, it is clearly stated "Whether you report allegations via the online complaint form, phone, fax, mail, e-mail, or in person, OIG will not disclose your identity without your consent, unless the Inspector General determines such disclosure is unavoidable during the course of the investigation."
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals/employess have an opportunity to decline to provide PII/BII.	Specify how: For OIG's Human Resources Management Division, individuals could decline to provide PII but that would severely impair the individual's ability to receive human resource services. For OIG's Office of Investigations, while it is Departmental policy

		that all Department employees shall fully cooperate with and provide information to the OIG, under certain circumstances the subject of an investigation cannot be required to supply information to the investigators.
	No, individuals do not have an opportunity to decline to provide PII/BII.	

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

x	Yes, individuals/employees have an opportunity to consent to particular uses of their PII/BII.	Specify how: For information provided to OIG's Human Resources Management Division, individuals have the opportunity to consent to particular uses of PII/BII through HR Connect, a Department level program.
x	No, individuals/employees do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: For records covered by OIG Office of Investigations, system of records notification, individuals do not have an opportunity to consent to particular uses of their PII/BII provided the use is a routine use of the records maintained in the system as described in the OIG's System of Records Notice.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals have an opportunity to review/update some records pertaining to them under the Privacy Act, 5 U.S.C. § 552a(d). Department of Commerce regulations describing the procedures for such access are at 15 C.F.R. Part 4, Subpart B. For information provided to OIG's Human Resources Management Division, individuals have the opportunity to update and review particular uses of PII/BII through HR Connect, a Department level program.
x	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: For OIG's Office of Investigations, individuals do not have an opportunity to review/update PII/BII pertaining to them under exemptions (j)(2) and (k)(2) of the Privacy Act of 1974, 5 U.S.C. § 552a: **(j) General Exemptions** - The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is— (2) maintained by an agency or component thereof whichperforms as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probationstatus; (B) information compiled for the purpose of a criminal

		investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision. **(k) Specific exemptions**.--The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is— (2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all thatapply.)*

x	All users signed a confidentiality agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to PII/BII is restricted to authorized personnel only.
x	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access to Investigative and Data Loss Prevention Tools is monitored, tracked, and recorded through audit logs maintained by the respective tools that record the user, user action, time of user action, and whether user action was successful or not as baseline auditing. If necessary due to anomalies, spikes, or any other causes for concern; additional audit data can be captured.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization: 09/30/2017
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is moderate.
x	NIST 800-122 recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the ITsystem.

Currently, ForcePoint Data Security is used to scan Data, Email, and Web access both inbound and outbound for any traffic containing PII coming in to the OIG. Any email found to contain sensitive PII is quarantined, not released, and marked for deletion. Additionally, new software, (e.g. Varonis) scans to detect any modification, alteration, attempts to delete, or relocation to a non-secure site of any document containing sensitive PII.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice. Provide the system name and number: Privacy Act records are covered by existing Department SORNs, including COMMERCE/DEPT-12, OIG Investigative Records and COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies. The OIG is also drafting an additional SORN that we anticipate will apply to certain data analytics records.
	Yes, a system of records notice has been submitted to the Department for approval on (date).
	No, a system of records is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. Check all that apply.

x	There is an approved record control schedule. Provide the name of the record control schedule: The Office of Inspector General has eight (8) records control schedules: Office of the Inspector General, Immediate Office of the Inspector General (https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-commerce/rg- 0040/n1-040-10-002_sf115.pdf) Office of the Inspector General, Office of Counsel (https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-commerce/rg- 0040/n1-040-10-001_sf115.pdf) Office of Inspector General, Office of Investigations Records Schedule (https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-commerce/rg- 0040/n1-040-02-001_sf115.pdf) Office of Inspector General Inspections and Program Evaluations (https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-commerce/rg- 0040/n1-040-01-002_sf115.pdf) Office Inspector General, Office of Audits (https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-commerce/rg- 0040/n1-040-00-001_sf115.pdf) Inspector General Semiannual Report to Congress (https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-commerce/rg- 0040/daa-0040-2015-0002_sf115.pdf) Office of Audit and Evaluation, OIG, DOC, Audit/Evaluation File Management System (https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-commerce/rg- 0040/daa-0040-2016-0001_sf115.pdf) Office of Investigations, OIG, DOC, Case Management System (https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-commerce/rg-0040/daa-0040-2018-0001_sf115.pdf)

	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
x	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	x	Overwriting	
Degaussing		Deleting	**X**
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
x	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets,

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Identification of specific individuals is required to provide HR services, administrative services, as well as for investigation.
X	Quantity of PII	Sufficient quantity is collected to pinpoint correct individuals for providing services as well as for investigation. Also, several years of PII data is stored and archived as required by law
X	Data Field Sensitivity	Multiple types of sensitive information including general personal data and work related data are collected.
X	Context of Use	PII/BII may be incidentally collected for audits and investigations and internally for administrative purposes.
X	Obligation to Protect Confidentiality	OIG is legally obligated to protect PII.
X	Access to and Location of PII	Access controls are in place. Access to sensitive information is restricted and stored in a location that is monitored.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.