Version Number: 01-2017

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
OS-18 IT Infrastructure System

Reviewed by: WESLEY FRAVEL Digitally signed by WESLEY FRAVEL DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=WESLEY FRAVEL, 0.9.2342.19200300.100.1.1=13001003618524 Date: 2018.09.21 15:30:10 -04'00' _____, Bureau Chief Privacy Officer

☑ 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: 2018.09.28 18:49:59 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
Office the Secretary / IT Infrastructure System

Unique Project Identifier: OS-18

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

(b) System location
Herbert C. Hoover Building (HCHB)

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
SecurityManager (SM) connects to and exchanges data with other systems from the Department of Justice (DOJ) and the Office of Personnel Management (OPM) as described below:

Interconnection with DOJ

- Communication between the systems is via dedicated encrypted email connection that can only send and receive messages between DOJ and OSY. Fingerprints are emailed to DOJ and the results of the fingerprint checks are emailed to OSY.

Interconnection with OPM

- OS-018 has an interconnection with OPM via IBM's Connect Direct which is a secure file transfer. Encryption ensures that only OPM and DOC can communicate – the following systems transfer information via this method:
    - Office of Personnel Management (OPM) Investigative Report Management Functionality (IRMF) Electronic Delivery (eDelivery) that provides DOC with investigative results (reports) for a requested Personnel Security Investigation (PSI) to their identified adjudication organization. This interface is fully automated.
    - OPM Personnel Investigations Processing System (PIPS) Daily Case Status Data import that provides the status of ongoing investigations requested by Department of Commerce (DOC). This interface is fully automated.
    - Export of clearance information to OPM Central Verification System (CVS). This interface is not automated, the user requests machine readable output file that is subsequently imported into OPM CVS.

- OPM Electronic Questionnaire for Investigations Processing (e-QIP) import is an automated import of XML file as part of the eDelivery. It can also be downloaded separately from OPM and imported into SM manually by the user.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

The SecurityManager of the Department of Commerce is a OSY-wide web-based case management application designed to support the lifecycle of the DOC personnel security, administrative security, and classified visit management programs. The SecurityManager system provides the Department's security and responsible bureau personnel:

- A tool to quickly initiate, track, review, and/or complete the Department's pre-appointment, suitability/fitness determination, initial security clearance, reciprocity and reinvestigation processes.
- A tool to quickly log, track, reassign, and account for the Department's classified information.
- A tool to effectively and efficiently process the Department's Foreign National Visitors and Guests as prescribed in DAO 207-12, Titled: Foreign Access Management Program
- An interface with internal and external systems to exchange the data in secure and reliable manner. The 'internal exchange' is solely between two of the applications encompassed in OS18; Security Manager and Zylab. OS18 does not exchange data internally outside of OS18.

Typical transactions are accessing applications in the Security Manager, Civil Applicant System (CAS), Zylab (a DOC system), and Administrative Programs. The modules in Security Manager electronically collect the Social Security Number (SSN), passport information, date of birth, and place of birth of employees, foreign nationals, consultants, interns, volunteers, and contractors. The information is used to obtain clearance adjudication, dates of security briefings, and visitor requests for Foreign Nationals. This information is collected from the OPM Standard Forms (SF) 85, 85P, 86, and 86C which are completed and released by the individual for investigation and submitted electronically to OPM. Electronic submission to OPM is the only format that can be used to collect the data. The Foreign National visitor information is collected from the visitor by their sponsor and is submitted using the OSY Foreign National Visitor Request Form. The completed and released SFs (85, 85P, 86, and 86C) are provided electronically, through OPM's electronic Questionnaire for Investigations Processing system and submitted to the Department's OSY and Office of Human Resources Management (OHRM). A portion of the information collected is provided in the Security Manager derived from the SF-86 Questionnaire for National Security Positions, SF-86C Standard Form 86 Certification, SF-85 Questionnaire for Public Trust Positions, and SF-85P Questionnaire for Non-Sensitive Positions. A completed SF contains Personally Identifiable Information (PII) (verified by Security Specialist), such as Education,

Passport Information, Citizenship, Residency, Employment, Selective Service, Military History, People Who Know You, Marital Status, Relatives, Foreign Contacts, Foreign Activities, Foreign Business, Foreign Travel, Police Record, Investigations and Clearance Information, Financial Record, Use of Information Technology, Involvement in Non-Criminal Court Actions, and Associations.

CAS collects and submits fingerprints and individual information such as eye color, weight, height, and hair color, using the SF-87 OPM Finger Print Card, to the DOJ's Joint Automated Booking System Division via encrypted email to confirm the legitimacy of the information.

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

SecurityManager provides access to the data via the internet browser user interface. The access is strictly enforced by authentication and authorization scheme.

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

OPM PIPS Daily Case Status files and eDelivery Distributed Investigative Files (DIF), including e-QIP XML file, are transferred from OPM to DOC server hosting Connect:Direct Secure Plus communication software node to SecurityManager (SM) web server. Then the files are picked up by SMeDelivery windows service and processed. The documents are registered in SM database and placed on designated folder. Currently the destination folder is on web server. Documents are encrypted in transport and at rest. All manual export/import files, such as Central Verification System (CVS) export and National Finance Center (NFC) import, are handled by the user. The application export/import module prompts the user for file location during the export or import process. These files are not encrypted and user is responsible for handling them, including deletion, per DOC policy.

(g) Any information sharing conducted by the system

The information is required and only shared with OPM for the selected positions to provide personal information for the required background investigations, reinvestigations, and continuous evaluations for employment or affiliation with the Department, in accordance with 5 CFR 731, 5 CFR 732, Executive Orders (EO) 10450, 12968, 13488, 13467. Fingerprints are shared with FBI (DOJ) to conduct background checks and provide advice to DOC.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

- Executive Order (EO) 9397, Numbering System for Federal Accounts Relating to Individual Persons, as amended by EO 13478, Amendments to EO 9397 Relating to Federal Agency Use of Social Security Numbers.

- EO 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information.
- EO 10577, Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service.
- Title 5, Code of Federal Regulations, Part 731, Suitability;
- Title 5, Code of Federal Regulations, Part 732, National Security Positions;
- The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, codified in Executive Order 13381 (6-27-05). The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, codified in Executive Order 13381, mandates that agencies ensure the appropriate uniformity, centralization, efficiency, effectiveness, timeliness, and reciprocity of determining eligibility for access to classified national security information. Centralization and automation of related data as described here directly supports this mandate.
- Executive Order (E.O.) 12968, as amended, "Access to Classified Information," August 2, 1995
- National Security Affairs Memorandum, "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," December 29, 2005
- E.O. 10450, as amended, "Security Requirements for Government Employment," April 27, 1953
- U.S. Department of Commerce (DOC) Department Administrative Order (DAO) 207-12, Titled: Foreign Access Management Program

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

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.
_____ This is an existing information system with changes that 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):					

__X__ This is an existing information system in which changes do not create new privacy risks.

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*	X	e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: The individual's SSN is collected to verify the individual's identity, required/needed for investigation/reinvestigations through OPM and to pass clearance information to other Federal Agencies.					

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		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): Citizenship, Former Residency, Employment, People Who Know You, Marital Status, Relatives, Foreign Contacts, Foreign Activities, Foreign Business, Foreign Travel, Police Record, Investigations and Clearance Information, Use of Information Technology, Involvement in Non-Criminal Court Actions, and Associations					

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X	d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos	X	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		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)
To assist in the auditing of Security Manager, OCIO is using the software Logmeister which monitors Windows event logs, syslog and text logs on servers throughout the network. Logmeister provides immediate notification of key events so that systems administrators can take appropriate and timely action. Logmeister also consolidates, archives, transforms and exports the log data for reporting.

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

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

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

A large portion of information collected for and maintained by the system is collected directly from the individual to whom it pertains via standard forms or electronic submission as outlined in introductory sections d and f, as well as Section 7 of this PIA. As such, information is generally considered to be accurate, relevant, and timely. That said, information is also reviewed for accuracy by using weekly and monthly reports to analyze the information for errors and inconsistencies.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. SF-85P – Questionnaire for Public Trust Positions: OMB No. 4206-0191 SF-85 – Questionnaire for Non-Sensitive Positions: OMB No. 3206-0261

	SF-86 – Questionnaire for National Security Positions: OMB No. 3206 0005 SF-86 – Questionnaire for National Security Positions (Certification): OMB No. 3206-0005 OSY Form 207-12, Form A – DOC Foreign National Request Form: OMB No. Pending Approval
	No, the information is not covered by the Paperwork Reduction Act.

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

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		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There is not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

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

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
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):			

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).

Security Manager: The modules in Security Manager electronically collect Social Security numbers, passport information, birthdates, and place of birth of employees, foreign nationals, consultants, interns, volunteers, and contractors. The information is used to obtain clearance adjudication, dates of security briefings, and visitor request for Foreign Nationals. The data is maintained in the system as a system of record and to verify existing data.
CAS: The information is collected from members of the public who are seeking employment or affiliation with the Department then disseminated to DOJ for the individual background checks. The data is used to determine if working with the Department is viable. The information collected is stored as historical data for one month.
ZyLab: The information is collected from federal employees and contractors to be used for the adjudication process. Once adjudication is determined, the individuals' personal information is archived as part of the personnel security procedures to support criminal investigations.
Administrative Programs: The information is collected from OSY's federal employees and invitational travelers. The data is used for travel orders, training, and tracking governmental property. The information is maintained as historical data for three years.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit 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.)

There is a risk that information in the system could be misused: The system has assigned roles for each user, as well as processes and procedures in place to manage access and system permissions. Each bureau is required to complete an access form for new personnel needing access to the system. OSY verifies the investigation level and sets the roles according to the user's needs. Further, the mandatory investigation needed to provide access to a user is a Tier 2. All DOC users are subject to signing and abiding by an Access and Use policy (i.e. a "Rules of Behavior") for access to and use of DOC systems and the information processed on them. Signing the Access and Use policy is a precondition for being granted access to DOC IT systems and users must also take mandatory training prior to being granted access to IT systems. Further, users must take annual refresher training in order to maintain access to IT systems. Additionally, DOC uses software to monitor system and server event logs for malicious or unusual activity. Finally, DOC has implemented a Data Loss Protection (DLP program to identify potentially unauthorized or unsecured disclosures of sensitive PII.

There is risk that information in the system could be breached, lost, compromised, or otherwise subject to unauthorized disclosure or exposure: To reduce the risk of information or system compromise, DOC employs appropriate security controls for the system in accordance with NIST 800-53, as described in Section 8.1 below. Additionally, DOC provides information security awareness training at the point of employee onboarding and mandates all end-user's complete refresher information security awareness training on an annual basis. Further, users sign an Access and Use policy (i.e. a "Rules of Behavior") for access to DOC systems. Finally, the system is subject to regular monitoring by administrators as described above.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

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			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

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

X	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: OS-018 has an interconnection with DOJ. Communication between the systems is via dedicated encrypted email connection that can only send and receive messages between DOJ and OSY. OS-018 has an interconnection with OPM via IBM's Connect Direct which is a secure file transfer. Encryption ensures that only OPM and DOC can communicate.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII 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 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: .	
X	Yes, notice is provided by other means.	Specify how: **Security Manager** – Individuals are notified by forms that collect the information. The forms used are SF-85 Questionnaire for Non-Sensitive Positions, SF-85P Questionnaire for Public Trust Positions, SF-86 Questionnaire for National Security Positions, and SF-86C Standard Form 86 Certification. **Zylab** – Individuals are notified by forms that collect the information. The forms used are SF-85 Questionnaire for Non-Sensitive Positions, SF-85P Questionnaire for Public Trust Positions, SF-86 Questionnaire for National Security Positions, and SF-86C Standard Form 86 Certification. **CAS** – Individuals are notified by the SF-87 (OPM Fingerprint Card) at time of fingerprint collection. **Administrative Programs** – Individuals are notified through the use of a warning banner prior to logging into the application.

	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 have an opportunity to decline to provide PII/BII.	**Security Manager** – The servicing Human Resources Specialist informs the individual that providing information is voluntary. Not providing the PII information may prevent completion of the investigation. Selected individuals for employment have the opportunity to decline to provide the requested information within Security Manager by not submitting the information to OPM, which will impede eligibility for the position selected. The forms used are the SF-85 Questionnaire for Non-Sensitive Positions, SF-85P Questionnaire for Public Trust Positions, SF-86 Questionnaire for National Security Positions, and SF-86C Standard Form 86 Certification. **Zylab** – PII collected as a result of the investigation is captured for archival purposes only. Individuals selected for employment have the opportunity to decline to provide the PII information by not completing the investigation forms listed. **CAS** – Individuals have the opportunity to decline to provide the requested PII by not submitting it, which will impede their employment eligibility. **Administrative Programs** – Individuals may decline to provide PII / BII after viewing the warning banner and at any time during data entry. They may decline to provide requested PII, however it will delay / deny the processing of their training and / or travel requests.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: **Security Manager** – When an individual completes the SF-85 Questionnaire for Non-Sensitive Positions, SF-85P Questionnaire for Public Trust Positions, SF-86 Questionnaire for National Security Positions, and SF-86C Standard Form 86 Certification, he / she consents that the PII information collected may be disclosed. The information is uploaded into Security Manager. **Zylab** – When an individual completes the SF-85 Questionnaire for Non-Sensitive Positions, SF-85P Questionnaire for Public Trust Position, SF-86 Questionnaire for National Security Positions, and SF-86C Standard Form 86 Certification he / she consents that the PII information collected may be disclosed. This information is uploaded into ZyLab.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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: **Security Manager** – Individuals may contact the OHRM personnel or OSY to review or update their personal information within Security Manager. Upon completion of the SF-85 Questionnaire for Non-Sensitive Positions, SF-85P Questionnaire for Public Trust Positions, SF-86 Questionnaire for National Security Positions, and SF-86C Standard Form 86 Certification, the individual has the opportunity to review and update their PII prior to submission. Some investigations will include an interview with the individual. This provides the opportunity to update, clarify, and explain information that was provided from the individual. **ZyLab** – The information contained within ZyLab is for archiving documents collected only and is not updated, but information can be added when there is a request to update their investigation / clearance information. The information collected is found on the completed SF-85 Questionnaire for Non-Sensitive Positions, SF-85P Questionnaire for Public Trust Positions, SF-86 Questionnaire for National Security Positions, and SF-86C Standard Form 86 Certification. **CAS** – The results received from DOJ can be reviewed however, cannot be updated by the individual. **Administrative Programs** – Information collected within Administrative Programs is personally entered by the OSY employee for travel and training requirements. All updates can be performed by the employee either by editing the form and submitting the updated form to OSY, or by requesting medication verbally or in writing to OSY.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

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

	All users signed a confidentiality agreement or non-disclosure 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 the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 9/8/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.

X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
	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.
X	Other (specify): Contractors must have a favorable background investigation and complete the annual IT Security Awareness training.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

To reduce the risk to PII/BII on the system, DOC employs appropriate security controls for the system in accordance with NIST 800-53, as referenced in Section 8.1 above. Additional controls have been applied to the system in accordance with the DOC Privacy Overlay requirements for "High" confidentiality systems. Additionally, DOC provides information security awareness training at the point of employee onboarding and mandates all end-user's complete refresher information security awareness training on an annual basis. Further, users sign an Access and Use policy (i.e. a "Rules of Behavior") for access to DOC systems. Finally, the system is subject to regular monitoring by administrators via various tools employed within DOC. Included in these are a Data Loss Prevention (DLP) capability which monitors traffic for unauthorized or unsecured disclosures of sensitive PII.

Additionally, OS-018 has an interconnection with DOJ and OPM. For the connection to DOJ, communication between the systems is via dedicated encrypted email connection that can only send and receive messages between DOJ and OSY. Only authorized OSY personnel have access to PII. Data is maintained and encrypted at rest on the system. For the interconnection with OPM, connection is made via IBM's ConnectDirect which is a secure file transfer. Encryption ensures that only OPM and DOC can communicate.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.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 (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/DEPT-9 – Travel Records, (Domestic & Foreign) of Employees and Certain Other Persons

	http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-9.html COMMERCE/DEPT-13 – Investigative and Security Records http://www.corporateservices.noaa.gov/audit/privacy_act/systems-of-records/commerce-department-13.html COMMERCE/DEPT-16 – Property Accountability Files http://www.corporateservices.noaa.gov/audit/privacy_act/systems-of-records/commerce-department-16.html COMMERCE/DEPT-18 – Employees Personnel Files Not Covered by Notices of Other Agencies http://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

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: General Records Schedule 3 – Procurement, Supply, and Grant Records, General Records Schedule 9 – Travel and Transportation Records & General Records Schedule 18 – Security and Protective Services Records.
	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	X	Deleting	X
Other (specify):			

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

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. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

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

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

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

X	Identifiability	Provide explanation: PII data can directly identify individuals.
X	Quantity of PII	Provide explanation: System contains large PII datasets.
X	Data Field Sensitivity	Provide explanation: PII data fields contain sensitive PII data.
X	Context of Use	Provide explanation: PII data is for conducting background investigations / verifications on individuals.
X	Obligation to Protect Confidentiality	Provide explanation: System has obligations to protect the confidentiality of PII data.
X	Access to and Location of PII	Provide explanation: PII data can only be accessed by authorized personnel.
	Other:	Provide explanation: N/A

Section 12: Analysis

12.1 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. Also, describe the choices that the bureau/operating unit 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.)

There is a risk associated with the collection and processing of sensitive information by the system: Information collected for and maintained within the system includes sensitive PII, including Social Security numbers and biometric information. As such, the DOC has employed technical and administrative controls for the system in accordance with guidance outlined in NIST 800-53, Revision 4, as well as additional controls for a "High" confidentiality system in accordance with the DOC Privacy Overlay. DOC limits access to the system to a small number of authorized users, approved by OSY, with specific user roles and system permissions. The system is regularly monitored for misuse by administrators.

Regarding data collected for and processed by the system, data points were determined in accordance with Federal standards for conducting background investigations and similar checks related to personnel and physical security. Data points align to Standard Forms used across the government for granting access to information or facilities for employees, contractors, staff, and visitors. Data is provided by individuals seeking employment with DOC or access to DOC facilities. Opportunities to consent to the collection and use of this information, and to access, amend and correct such information exist.

12.2 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.

12.3 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.