Version Number: 01-2015

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
OS-018 IT Infrastructure System

Reviewed by: Michael J. Toland, Office of the Secretary (OS) 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 D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2016.09.29 17:06:04 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
OCIO/OITS OS-018 IT Infrastructure System

Unique Project Identifier: OS-018

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) a general description of the information in the system

The Office of Security (OSY) IT Infrastructure Accreditation Boundary is encompassed within the Herbert C. Hoover Building (HCHB) Data Center. The IT Infrastructure system includes servers, other hardware components, operating system boundary because they are owned by another Federal agency. Direct Connect is owned by Office of Personnel Management (OPM), and Civil Applicant Service is owned by Department of Justice (DOJ). Memorandums of Understanding (MOUs) are in place with these two agencies.

(b) a description of a typical transaction conducted on the system

Typical transactions are accessing applications in the *Security Manager*, *Civil Applicant System (CAS)*, *Zylab*, 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 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 provided by the incumbent (employee/contractor/affiliate) who received the conditional job/affiliation offer. Fingerprint information collected from the applicant is collected within OSY and sent to DOJ for review. The results are then received from DOJ for use in adjudicating applicant. Information is transmitted using a dedicated encrypted email connection that can only send and receive messages between DOJ and OSY. There are no other connections to or from the system. The applicant's fingerprint request and subsequent results are deleted from the system within one month of receipt.

The adjudication records collected are scanned and archived in *Zylab*. The archived information in Zylab is reviewed by the OSY Security Specialist to analyze questions related to the adjudication or an audit.

Administrative Programs store electronic information necessary to complete travel and training forms and used to track OSY's government property. This information is stored for archived purposes. 41 CFR, Subtitle F – Federal Travel Regulation System Chapters 300 through 304 and OMB Circular A-123 – Management's Responsibility Internal Control. Also, OSY will send PII from Security Manager to all Federal agencies that request the information for clearance verification.

(c) 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.

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

5 CFR 731, 5 CFR 732, Executive Orders (EO) 10450, 12968, 13488, 13467. 41 CFR, Subtitle F – Federal Travel Regulation System Chapters 300 through 304 and OMB Circular A-123 – Management's Responsibility Internal Control.

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system

The OSY Infrastructure system encompasses the applications identified in the statements above. The system supports the accomplishment of OSY's mission goals and objectives, which include ensuring that OSY employees have the tools (hardware, software, and training) and access the internal and external information resources necessary to perform their responsibilities, ensuring the availability of work products and information, and satisfying mission-oriented data processing requirements in a timely and cost-effective manner. The regional OSY field units and supported bureaus need to have the capability to communicate readily with OSY headquarters for accessing business essential and mission critical application programs. The security categorization 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.
_____ This is an existing information system with changes that create new privacy risks.
__X__This is an existing information system there are no 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): This PIA was performed as part of the information system's annual review.					

x_ This is an existing information system for which there is not a recent PIA

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): Employment History					

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): Eye color, hair color, height, weight.					

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)

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	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	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 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 are 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			
To determine eligibility	X	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 / 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.

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.
	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.	Specify how: 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 for. 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 above. 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.

		CAS – Individuals consent to the use of CAS by choosing to provide their fingerprints on the SF-87 (OPM Fingerprint Card). Administrative Programs – Individuals consent to the use of PII when they click "OK" on the warning banner which provides information concerning the use of their PII. They also consent to its use when the individual enters the necessary information into the Administrative Programs application.
	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): _TBD_____ ☐ 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 (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.
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.

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. Only authorized OSY personnel have access to PII. Data is maintained and encrypted at rest on the system.

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 and number *(list all that apply)*: Department 9 – Travel Records, (Domestic & Foreign) of Employees and Certain Other Persons, Department 13 – Investigative and Security Records, Department 16 – Property Accountability Files, Department 18 – Employees Personnel Files Not Covered by Notices of Other Agencies.
X	Yes, a SORN has been submitted to the Department for approval on (date). 6/14/2016
	No, a SORN 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: 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 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.
	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:

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.