Version Number: 01-2020

U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis
for the
OS-018 IT Infrastructure System

U.S. Department of Commerce Privacy Threshold Analysis
Office of the Secretary/IT Infrastructure System

Unique Project Identifier: OS018

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based on the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed to complete this PTA, please contact your Bureau Chief Privacy Officer(BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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 (DOD), and Civil Applicant Service (CAS) is owned by Department of Justice (DOJ). Memorandums of Understanding (MOUs) are in place with these two agencies.

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

b) *System location*
Department of Commerce (DOC) Headquarters at the Herbert C. Hoover Building (HCHB) 1401 Constitution Avenue, NW
Washington, DC. 20230

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 Department of Defense (DOD) 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 DOD

OS-018 has an interconnection with DOD via IBM's Connect Direct which is a securefile transfer. Encryption ensures that only DOD and DOC can communicate – the following systems transfer information via this method: Department of Defense (DOD) 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.

- DOD 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 fullyautomated.
- Export of clearance information to DOD Central Verification System (CVS). This interface is not automated, the user requests machine readable output file that is subsequently imported into DOD CVS.
- DOD 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 DOD and imported into SM manually by the user.

d) The purpose that the system is designed to serve.

The purpose of Security Manager is to support the lifecycle of the DOC personnel security, administrative security, and classified visit management programs.

e) The way the system operates to achieve the purpose.

The SecurityManager of the Department of Commerce is an 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 Security Manager 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 Admin 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 Fingerprint Card, to the DOJ's Joint Automated Booking System Division via encrypted email to confirm the legitimacy of the information.

f) A general description of the type of information collected, maintained, use, or disseminated by the system.

The system collects personal information to enable the adjudication of fitness for employment.

g) Identify individuals who have access to information on the system.

Government employees and contractors have access to the information on the system.

h) 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.

i) How information is transmitted to and from the system

DOD 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.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and completecertification.*

_____ This is an existing information system with changes that create newprivacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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 is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

__X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017). *Continue to answer questions and completecertification.*

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

_____ Yes. This is a new information system.

_____ Yes. This is an existing information system for which an amended contract is needed.

_____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

__X_No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

_____ Yes. *(Check all that apply.)*

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

_X____No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

_____ Yes, the IT system collects, maintains, or disseminates BII.

__X___No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

__X__Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__DOC employees
__X__Contractors working on behalf of DOC
__X Other Federal Government personnel
__X__Members of the public

_____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

__X__Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form. a. SecurityManager is used to store and maintain PII necessary to identify an individual and to track completion of suitability and national security related processes, including background or other investigations concerning the individual. b. Civil Applicant System (CAS) stores and maintain fingerprint result data is used to assist DOC in the fitness and suitability for onboarding process.
Provide the legal authority which permits the collection of SSNs, including truncated form. a. Executive Order 13467, as amended b. Defense Counterintelligence and Security Agency (DCSA) c. Under title 5, Code of Federal Regulations, part 731 (5 CFR 731)

_____ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than userID.

_____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

_____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above apply to the OS- 018 IT Infrastructure System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____I certify the criteria implied by the questions above **do not apply** to the OS-018 IT Infrastructure System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Kevin Mills Office: OS/OIPS Phone: 202-482-2779 Email: KMills@doc.gov Signature: KEVIN MILLS Digitally signed by KEVIN MILLS Date: 2021.04.12 14:34:29 -04'00' Date signed:	**Information Technology Security Officer** Name: Jerome Nash Office: OS/OSSD Phone: 202-482-5929 Email: JNash@doc.gov Signature: JEROME NASH Digitally signed by JEROME NASH Date: 2021.04.03 14:59:54 -05'00' Date signed:
Privacy Act Officer Name: Tahira Murphy Office: OPOG Phone: 202.482.8075 Email: TMurphy2@doc.gov Signature: TAHIRA MURPHY Digitally signed by TAHIRA MURPHY Date: 2021.09.29 19:15:38 -04'00' Date signed:	**Authorizing Official** Name: Lawrence W. Anderson Office: Office of the Secretary Phone: 202-482-2626 Email: LAnderson@doc.gov Signature: LAWRENCE ANDERSON Digitally signed by LAWRENCE ANDERSON Date: 2021.04.04 11:18:08 -04'00' Date signed:
Bureau Chief Privacy Officer Name: Maria D. Dumas Office: OPOG Phone: 202-482-5153 Email: MDumas@doc.gov Signature: MARIA STANTON-DUMAS Digitally signed by MARIA STANTON-DUMAS Date: 2021.09.29 23:37:28 -04'00' Date signed:	