

**U.S. Department of Commerce  
Office of the Secretary**



**Privacy Threshold Analysis  
for the  
OS-18 IT Infrastructure System**

## U.S. Department of Commerce Privacy Threshold Analysis

### OS-18 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 from 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 in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

**Description of the information system and its purpose:** *Provide a general description of the information system in a way that a non-technical person can understand.*

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 (OPM), 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*

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:

- o 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.

- o 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.
- o 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.
- o 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 purpose that the system is designed to serve*

The purpose of SecurityManager 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 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.

*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*

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.

### **Questionnaire:**

1. What is the status of this information system?

\_\_\_\_\_ This is a new information system. *Continue to answer questions and complete certification.*

\_\_\_\_\_ This is an existing information system with changes that create new privacy 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 later). *Skip questions and complete certification.*

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. *Please describe the activities which may raise privacy concerns.*

  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 about: *(Check all that apply.)*

\_\_\_\_\_ Companies

\_\_\_\_\_ Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

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

DOC employees

Contractors working on behalf of DOC

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 PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

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

4c. 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.

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, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.***

