Version Number: 01-2017

U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis
for the
Physical Security System

U.S. Department of Commerce Privacy Threshold Analysis

Office of Security, Physical Security System

Unique Project Identifier: OS-043 – Physical Security System

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).

a) *Whether it is a general support system, major application, or other type of system*
General Support System (GSS).

b) *System location*
The Physical Security System (PSS) is located within the 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)*
The PSS is a stand-alone system and does not interconnect with systems outside of its boundaries.

d) *The purpose that the system is designed to serve*
The PSS consists of several components that provide an approach to securing and monitoring the physical aspects of the HCHB, the Department of Commerce's (DOC) primary facility. The system supports video monitoring, alarm monitoring, building access control, and emergency preparedness.

e) *The way the system operates to achieve the purpose*
The PSS supports the Department of Commerce's (DOC) primary facility, the HCHB, by utilizing two subsystems. The information system has been divided into the following functional areas: Closed-Circuit Television (CCTV) and Physical Access Control System (PACS). The details of the sub-systems are provided below.

1. Closed-Circuit Television (CCTV)

The Closed-Circuit Television (CCTV) functional area encompasses all video equipment used to monitor the HCHB. This includes the digital video recorders (DVRs) that capture and record video streams coming from the video cameras. The main Guard Office monitors the video from these cameras. Monitors receiving input from these cameras are also placed at selected guard stations throughout the building. CCTV serves as the eyes of the HCHB. This system is meant for occupant emergency procedures and to detect and deter unauthorized activities in accordance with Department of Homeland Security Interagency Security Committee Risk Management Processes for Federal Facility Standards and associated recommended Physical Security Levels of Protection. DOC CCTV provides security detection measures that meet the NIST 800-53 Rev.4 Physical Security family control PE-5 – Monitoring Physical Access. The DOC Security Office places security cameras around the perimeter and inside HCHB facilities to include the Childcare Center playground, the garage, building exits, common areas and outside of secured areas. HCHB uses the video feeds captured through CCTV for security and law enforcement purposes. Implementing this control ensures that physical access to HCHB information systems is monitored to detect and respond to physical security incidents, while providing results to review for investigations. These results are coordinated with the Security Shared Services (S3) Operating Unit's (OU's) incident response capability. This statement of purpose meets the privacy control AP-2 – Purpose Specification for CCTV. Per requirements for the security control AC-3 – Access Enforcement, the PSS is in compliance with HCHB S3 ITSP having its role-based access implemented for groups in ProWatch utilizing the Active Directory.

2. Physical Access Control System (PACS)

Physical Access Control System (PACS) includes all software, hardware, and firmware (software that is embedded in a piece of hardware) that participate in the management or operation of physical access to the HCHB. The heart of this component is the Access Control Software (ACS). The ACS is used to manage and monitor all designated areas where a badge authorizes entrance. Personal Identity Verification (PIV) cards are used for access into and within the HCHB by all authorized personnel. The ACS receives the Personally Identifiable Information (PII) on an employee requesting access from the employee's PIV card when their PIV card is scanned by a card reader at the door to a designated area. The ACS requires personnel to identify themselves before gaining authorization to that area. These card readers are hardwired directly to a central unit that mediates command and control information flowing between the card reader and the ACS.

The CCTV system records video from a variety of ranges and with differing zooming capabilities. The cameras record passersby on public streets and HCHB employees, contractors and visitors accessing the facility. CCTV cameras collect video images through real-time monitoring with streaming and storage onto a storage device. Zooming capability allows for the recording of textual information such as license plate numbers. Cameras contain low-light technology to support detection of unauthorized or suspicious activities at

night. Most cameras are fixed but others use pan/tilt/zoom capability with manual tracking, which allows the individual monitoring the CCTV feed to adjust the camera in real time to gain the best image of any suspicious or illegal activity of interest that is occurring.

With regards to the PACS, a typical transaction begins when a Badge Access Control administrator creates a Personal Identity Verification or "PIV" card for an individual. The PIV card includes the employee's name and photograph, as well as information about building access privileges. The card is provided to the individual for access to the HCHB and certain information technology (IT) resources. When the employee scans their PIV card on a card reader located at the door of a designated area, the ACS receives the information on the employee requesting access from their PIV card. The ACS then verifies the identity and the access privileges of the employee requesting access. Access to the designated area is either granted or denied depending on the employee's building access privileges.

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

Information processed by the BAC includes: DOC employee, contractors, detailees, interns, and other staff's names, position title, photograph and building access permissions, as well as information pertaining to entry into the HCHB and specific areas within the facility.

Information processed by the CCTV includes still and video images, including facial images, of DOC employees, contractors, detailees, interns, and other staff, as well visitors to the HCHB and members of the public in and around monitored areas of the HCHB, as well as images of license plates and other potentially identifying information about individuals in and around the HCHB.

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

Access to information processed by the PSS is limited to authorized members of the DOC Physical Security team, and other authorized officials on a need-to-know, case-by-case basis in relation to a physical security or law-enforcement related issue.

h) How information in the system is retrieved by the user

Retrieval of system information depends on the nature of the subsystem and the transaction occurring. For PACS, the system retrieves information about an employee and their access privileges at the time a PIV card is presented to a card reader at a designated area within the HCHB. User profiles and associated PIV information for each authorized user exists within the ACS. Each ACS transaction results in a record of accountability in which the system checks the PIV card against the existing profile database to authorize access providing that the parameters on the PIV match the parameters within the ACS database permissions for that card reader. Reports in ProWatch software can be generated to review access entries by individual, date, badge reader, access space, and clearance code. Only ACS authorized personnel with a need to know have access to retrieve these records and run reports.

For CCTV, still and video images and other information may be retrieved real-time by using the pan/tilt/zoom functions outlined above, or later, by reviewing recorded footage or images within a time or date range. Cameras are connected to a Network Video Recorder (NVR) interface, which allows interoperability for the storage and retrieval of video images. Only authorized OSY personnel with a need to know have access to the information. CCTV does not record or retrieve information by personal identifiers, only by date, time, and location. The video, which is not encrypted, is automatically overwritten every 120 days.

i) How information is transmitted to and from the system

As outlined above, the CCTV system records video from a variety of ranges and with differing zooming capabilities at various locations within the HCHB and on the surrounding premises. Recordings are then compressed via algorithm and stored on hard drives located within the HCHB. Cameras record images that are stored and retrieved as necessary from NVR's. The system does not connect to or share with other systems, however, in the event of an approved request for video in support of a law-enforcement activity, data may be transferred from the hard drives onto transferable media for use by law enforcement on a case-by-case basis

ProWatch software is used to manage and monitor all sensitive areas where a PIV badge authorizes physical entrance. The PIV badge readers are located at door entrances to restricted areas where personnel are required to identify themselves before gaining authorization to that area. These card readers are hardwired directly to a central unit that mediates command and control information flowing between the PIV badge reader and the ProWatch software. The user presents her/his badge to the badge reader that authenticates and authorizes the user from the ProWatch software communicated through isolated VLANs on the HCHB network.

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):					

__X__ 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.*

____ 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.

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

The system supports video monitoring and badge readers for building access control.

____ 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

__X__ 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..."

__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__ 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?

__X__ 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.

__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, 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.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the Physical Security Systems 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 [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Michelle Holland

Signature of ISSO or SO: MICHELLE HOLLAND Digitally signed by MICHELLE HOLLAND DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=MICHELLE HOLLAND, 0.9.2342.19200300.100.1.1=13001000374103 Date: 2018.08.03 13:15:33 -04'00' Date: 8/3/2018

Name of Information Technology Security Officer (ITSO): Jun Kim

Signature of ITSO: JUN KIM Digitally signed by JUN KIM DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=JUN KIM, 0.9.2342.19200300.100.1.1=13001001483988 Date: 2018.08.07 16:02:51 -04'00' Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: RODNEY TURK Digitally signed by RODNEY TURK DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=RODNEY TURK, 0.9.2342.19200300.100.1.1=13001002898461 Date: 2018.08.30 13:45:14 -04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Wesley Fravel

Signature of BCPO: 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: 2018.08.07 16:26:00 -04'00' Date: _____