Version Number: 01-2015

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
OSY Physical Security 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: 2016.10.07 17:57:32 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
Office of the Secretary (OS)
Office of Security (OSY) Physical Security System

Unique Project Identifier: OS-043

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 Physical Security System (PSS) supports the facility by utilizing two subsystems. The information system has been divided into the following functional areas: Closed Circuit Television (CCTV) and Building Access Control (BAC). The details of the sub-systems are provided below.

Sub-systems

Closed Circuit Television

The CCTV functional area encompasses all video equipment used to monitor the Herbert C. Hoover Building (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 is the eye 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.

Building Access Control

Building Access Control (BAC) includes all software, hardware, and firmware 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 employees, contractors, interns, affiliates and guests. 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 ACS monitors all alarm systems within the building.

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

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.

PIV cards are used for access into and within the HCHB by all employees, contractors, interns, affiliates and guests. A typical transaction conducted on the Building Access Control System begins when a Badge Access Control administrator creates a PIV card for an individual. The PIV card includes the employee's name, job title and photograph. This is given to the individual, and building access privileges information for that individual are also contained on the PIV card. When the employee scans their PIV card on the card reader located at the door to 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.

(c) any information sharing conducted by the system

CCTV and BAC system information sharing with other systems is prohibited. This system is stand-alone and does not interconnect with systems outside of its boundaries and is on a private VLAN. Local, state and federal government agencies may request copies of video that is captured by the system. Information from the CCTV cameras will be used by federal agencies and local law enforcement to detect and respond to potentially unlawful activities in real time in the areas surrounding federal facilities. The information may also be used to support law enforcement investigations and prosecutions to the extent it contains information relevant to a criminal or potentially criminal activity. For example, if a suspicious package is placed outside a federal building, the system would provide a real-time notification of this activity and allow federal officials or local law enforcement to take appropriate responsive action. Additionally, if the package is determined to be an explosive device, the recordings could be used to further investigate this criminal activity, assist in identifying the perpetrators, and/or provide evidence that may be used in court.

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

5 U.S.C. § 301, "Government Organization and Employees;"

Executive Order 12977, "Interagency Security Committee;"

Presidential Decision Directive 12, "Security Awareness and Reporting of Foreign Contacts;"

Homeland Security Presidential Directive-7, "Critical Infrastructure Identification, Prioritization and Protection;"

Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors;"

PIV of Federal Employees and Contractors FIPS 201-2;

National Infrastructure Protection Plan, "Government Facilities Sector, Sector-Specific Plan;"

The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, August 2013

Federal Property Regulations, July 2002. 1.2

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

FIPS 199 – 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): Updated PTA/PIA for OS-043					

__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*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		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:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	X	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		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)

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		Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
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	X
Video surveillance	X	Electronic purchase transactions	
Other (specify):			

	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		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	X
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): For badge access to the DoC HCHB building, and for video monitoring purposes.			

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).

CCTV: The information system contains images (still & video) of individuals who have authorized access (federal employees/contractors) to DOC HCHB building as well as members of the general public in the line of sight of internal and external cameras (members of the public, foreign nationals, and visitors). The data is used to detect and deter unauthorized individuals and activities and to ensure adequate levels of protection in accordance with Interagency Security Committee standards.

BAC: The information is collected from DOC federal employees, contractors, affiliates, guests and others as necessary via the DOC Personal Identity Verification (PIV) is used to create and authorize an individual with a badge which is used to access rooms in the HCHB equipped with a card reader. The information collected is to satisfy requirements specified in section 2.1 of FIPS 201-2: 'Personal Identity Verification (PIV) of Federal Employees and Contractors'.

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	X		
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.

	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:
X	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.

X	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: on the Request Forms CD-591 and OF-306.	
X	Yes, notice is provided by other means.	Specify how: BAC: Individuals are notified by their sponsor prior to filling out the DOC Personal Identity Verification (PIV) Request Form CD-591. OF-306 and Special Agreement Check (SAC) both contain Privacy Act Statements. The information collected is to satisfy requirements specified in section 2.1 of FIPS 201-2: 'Personal Identity Verification (PIV) of Federal Employees and Contractors'. CCTV: Notification is provided by signs stating that "Premises are under 24 hours recorded video surveillance".
	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: BAC: Individuals have the opportunity to decline to provide the requested PII collected by not submitting the DOC Personal Identity Verification (PIV) Request Form CD-591, OF-306 and SAC; however, this will impede their eligibility for a badge.
	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: BAC: When an individual completes the CD-591, OF-306 and SAC they consent that the PII information collected may be disclosed and used to provide HCHB access. This information is uploaded into the BAC 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: BAC: Information collected can be edited by requesting modification through 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): 9/8/2015 ☐ 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.

PSSis stand-alone and does not interconnect with third-party systems outside the control of DoC and is on a private VLAN. Only authorized OSY personnel have access to PII on OS-043. Data is maintain 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)*: COMMERCE/DEPT-13, Investigative and Security Records; COMMERCE/DEPT-25, Access Control and Identity Management System; GSA/GOVT-7, Personal Identity Verification Identity Management System (PIV IDMS).
	Yes, a SORN has been submitted to the Department for approval on (date).
	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 – Grant Records, General Records Schedule 9 – Travel and Transportation Records and 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		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: CCTV system contains images (still & video) of individuals who have authorized access to the HCHB as well members of the general public in the line of sight of external cameras. BAC contains Employee's name, job title and photograph.
X	Quantity of PII	Provide explanation: CCTV system contains continuous video recording of internal and external HCHB cameras. BAC system contains records of individuals who have authorized access to the HCHB.
	Data Field Sensitivity	Provide explanation:
X	Context of Use	Provide explanation: System contains records of individuals who have authorized access to the HCHB. CCTV is used to obtain real-time and recorded visual information in and around the HCHB to aid in crime prevention and criminal prosecution, enhance officer safety, secure physical access, and assist in terrorism investigation or terrorism prevention.
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 located within the HCHB.
	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.