Template Version Number: 01-2020

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
OS-043 Physical Security System

Reviewed by: Maria D. Dumas, Bureau Chief 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

Jennifer Goode 09/30/2021

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-043 Physical Security System

Unique Project Identifier: OS043

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) 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) 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 leverages OS-003 – HCHBNet as backbone infrastructure for connectivity and limited IT services associated with daily business functions of the PSS. The PSS is a stand-alone system and does not interconnect with systems outside of its boundaries.

(d) The way the system operates to achieve the purpose(s) identified in Section 4
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 RS2 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. There may also be vehicle identifiers via the use of CCTV, which includes license plate numbers derived from images of license plates for vehicles parked or driving within an area monitored by HCHB CCTV. 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.

(e) 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 RS2 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. Section 6.3 includes a detailed discussion of system access. 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, but may be retained longer if part of an active law enforcement activity, or if being maintained as a backup for disaster recovery purposes (up to 6 months).

(f) 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.

RS2 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 RS2 software. The user presents her/his badge to the badge reader that authenticates and authorizes the user from the RS2 software communicated through isolated VLANs on the HCHB network.

(g) Any information sharing conducted by the system

As noted above, the PSS relies on OS-003 – HCHBNet as its backbone infrastructure, but otherwise does not interconnect with systems outside of its boundaries. The system is on a private VLAN and information sharing with other systems is prohibited. Local, state, and federal government agencies may request copies of video 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.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The following statutes and executive orders authorize processing of information by the PSS:

- 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.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The PSS has been assigned a Federal Information Processing Standard (FIPS) 199 security impact category of 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. *(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 is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

_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).
____ 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).

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*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	X
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. 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	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address		s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address		i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs	X	j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify): Facial images of employees and visitors to the HCHB and surrounding areas monitored by CCTV.					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		f. Queries Run		f. Contents of Files	X
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 Describe how the accuracy of the information in the system is ensured.

Periodic, regular reviews are conducted by system administrative security specialists with a strict need-to-know. The database is reviewed quarterly to ensure that records are accurate; permissions deleted as necessary; badge expirations annotated and reviewed, and records archived as necessary. For CCTV, the cameras collect real-time video of the activities occurring within their viewing space in or near the HCHB. Videos are not altered or modified in anyway other than a compression algorithm which allows them to be stored in an array of hard drives, and there is no editing feature or ability to change or blur individual faces from the images captured For the PACS, employees are responsible for providing their information, via the DOC Personal Identity Verification (PIV) Request Form CD-591, the OF-306 and access is approved through the Special Agreement Check (SAC), which is used to grant access to the HCHB. Authorized personnel within the DOC Physical Security office are responsible for assigning access permissions to individuals based on the individual's position within DOC. Because information is collected directly from individuals it is generally assumed to be accurate, however, in cases where information is inaccurate, opportunities exist for access and correction by working with the OSY directly or via the Privacy Act procedures specific to the relevant SORN outlined in Section 9 of this PIA. Badge reader access logs are reviewed by OSY on a regular basis along with periodic audits to review whether permissions granted are accurate. Any discrepancies found in the reviews are corrected by OSY as follow up by restricting or granting proper PIV access to an individual.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.

X	No, the information is not covered by the Paperwork Reduction Act.

2.5 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			
For a Computer Matching Program		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):			

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 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.

PACS: The information is collected from DOC federal employees, contractors, affiliates, guests and others as necessary via the United States Federal smart card for DOC Personal Identity Verification (PIV). The PIV card contains the necessary data for the cardholder to be granted access to Federal facilities, information systems, and assure appropriate levels of security for applicable DOC federal applications. 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.'

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The primary risks posed by use of the PSS relates to data minimization and retention, and misuse or mishandling of data. Each is discussed in greater detail below.

There is a risk that the CCTV may collect unnecessary information, record more information than is necessary, or retain recorded information longer than is necessary. The purpose behind the use of a CCTV system for the HCHB is to detect and deter criminal activity and provide investigatory leads only. CCTV cameras do not record or transmit sound (i.e., audio). Additionally, access to the CCTV system and recordings is restricted to only a

small number of authorized individuals who monitor the video feeds or are granted access because of an investigatory or law-enforcement action. Access to the system is monitored and employees with access are subject to training, Code of Conduct, and background investigation requirements. Finally, video captured is subject to records retention requirements as discussed in this PIA and are overwritten after 120 days, unless authorized for extended retention as part of an ongoing law enforcement activity or as backed up for disaster recovery purposes (up to 6 months). The retention period is appropriately limited to only retain images for a short length of time, while still allowing DOC to identify potentially relevant video when a crime has occurred but is not immediately reported. Moreover, it aligns with NARA General Records Schedule (GRS) 5.6 Item 090, which deems routine video surveillance such as this to be "temporary" in nature and retained for a limited amount of time as is relevant to their purpose.

There is always the concern of insider threat. There is also a risk that the CCTV system or video or still images captured could be misused or mishandled.
As noted above, the CCTV system is only used to detect and deter criminal activity and provide investigatory leads as it relates to the HCHB. Access to the system and recordings is controlled and monitored and employees with access are subject to training, Code of Conduct, and background investigation requirements. Any sharing or use of information for law enforcement purposes must be approved by authorized DOC personnel. Additionally, all DOC personnel are required to take cybersecurity awareness training.

There is a risk that PACS system information could be misused or mishandled.
Only personnel who have a strict need-to-know and access to the system can access the information. Except for access reports as needed for security investigations by personnel with a strict need to know and issuance of identification/proximity and PIV badges, printing is generally not allowed for the system. Badges are produced and disseminated only to personnel who meet the characteristics of the information according to the badge profile within the system. Personnel are asked to produce a valid identification to the issuer prior to being issued a badge. All personnel gaining access to the system are provided training by OSY Technical Security personnel and the system is monitored by OSY Technical Security personnel to ensure that appropriate usage and procedures are being observed. Any personnel who are identified as using the system incorrectly will lose privileges and face administrative penalties, as necessary.

There is a risk that PACS could collect more information than is necessary.
This risk is minimal. Only the individual's name, bureau and business contact information are included, along with the long card number for the PIV, and the Proximity number for the DOC Blue or Red Badge. OSY made the decision to minimize the information within the badge profiles to the greatest extent possible. No date or place of birth, personal identification numbers (e.g., SSN or Employee ID) or individual characteristics are included within the database profile.

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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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: The PSS is supported by the HCHBNet (OS-003), which provides connectivity and limited IT services for the PSS and serves as an infrastructure backbone for the system. Sensitive information which traverses the HCHBNet includes hashed card numbers and access permissions between the PACs system and individual readers at the time a badge is presented to the reader for access to a restricted area within the HCHB, as well as video recordings from the cameras to the DVR which processes the recordings for display and review.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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): Access to the PSS is limited to OSY personnel with bona-fide need-to-know in support of their duties. For the PACs system, access is managed by three (3) individual administrators with advanced permissions (privileged users) or authority to approve accounts and grant permissions, to the RS2 software as necessary. After a request for access is approved by an administrator, users must have an account created and permissions assigned prior to logging into the system. Access is requested by filling out an access request form for the system and then providing that form to a supervisor, or, in the case of a contractor, the Contracting Officer's Representative (COR). These officials then provide senior DOC officials within OSY with the forms for approval. Once approved, OSY provides the form to system administrators via email and accounts are created and permissions assigned as appropriate. For the CCTV system, including the central area where DVRs are stored and recordings can be viewed, is controlled by card access and intrusion detection system(s) (IDS). As discussed earlier, card access is managed in the PACs system by authorized OSY personnel.			

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: Please see below.	
X	Yes, notice is provided by other means.	Specify how: PACS: Individuals are notified of the collection and use of their information by their sponsor prior to filling out the DOC Personal Identity Verification (PIV) Request Form CD-591, and again at the point of receiving their PIV card, where a Privacy Act Statement is presented and acknowledged. Both OF-306 and Special Agreement Check (SAC) 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 Contractor. CCTV: Notice is provided by signs stating that "Premises are under 24 hours recorded video surveillance."X
	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: PACS: 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, the OF-306, and SAC; however, not providing this information may result in being denied a PIV card and access to DOC facilities.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: CCTV: Individuals in and around monitored areas of the HCHB who are captured on video surveillance may not decline to have their PII/BII collected.

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: PACS: 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 access to the HCHB. As noted above, they may decline to provide information or consent to the collection and use of information but doing so may result in being denied a PIV card and/or access to DOC facilities.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: CCTV: Individuals in and around monitored areas of the HCHB who are captured on video surveillance may not consent to particular uses of their PII/BII

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: PACS: Individuals who submit information for issuance of a PIV or access to the HCHB may request modification of their information through the Office of Security. Additionally, individuals may be able to request access to or modification of their records via the Privacy Act request procedures outlined in the applicable SORNs outlined in Section 9 of this PIA. CCTV: Individuals in and around monitored areas of the HCHB who are captured on video surveillance may have limited opportunities to review PII/BII pertaining to them as captured in the system but may not update PII/BII pertaining to them as captured in the system. Review of video identifier information is limited because i) no personal identifiers are labeled in the images; ii) images cannot be altered in the system; and iii) video and images are automatically overwritten after 120 days unless deemed necessary for retention as part of an ongoing law enforcement activity or maintained as backups for disaster recovery purposes (up to 6 months).
	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.)*

X	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: As outlined in Section 6.3, access to the PSS is limited to OSY personnel (DOC employees and contractors) based on a strict need-to-know in performance of their specific duties. Access to the space where DVRs housing recordings from CCTVs is controlled and monitored by card access and IDS. Distribution of any recordings for law enforcement purposes must be approved by a specific senior member of the OSY team. Regarding the PACs system, the system is managed by three (3) individual administrators with advanced permissions (privileged users) who grant limited access to other users to the RS2 software as necessary. After a request for access is approved, account created and permissions granted by an administrator, use of the system is monitored by system administrators for abnormalities. Two (2) dedicated DOC employees are responsible for maintaining a list of contractors who support the OSY program and who have requested and been granted access to the PSS.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 08/25/2020 ☐ 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 (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
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 DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

PSS does not interconnect with third-party systems outside the control of DOC. The system is on a private VLAN and maintained within the DOC. Only authorized Office of Security personnel have access to the system and PII collected and maintained by the system. The PACS system is encrypted using RS2 Security Management Suite Architect and Engineering Specifications, 128-bit AES data encryption between the host and PW- 5000/PW-6000 intelligent controllers. The profile database which houses user profiles and associated PIV

information for each authorized user, and which the PACs system checks against when granting access is protected by FIPs 140-2 cryptographic modules. CCTV video is not encrypted.
The PSS systems employ a multitude of layered security controls to protect PII at rest, during processing, as well as The PSS systems also follow the National Institute of Standards and Technology (NIST) standards, including special publications 800-53, 800-63, and 800-37. Any system within the organization that contains, transmits or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. Finally, the organization also employs data loss prevention (DLP) solutions – the DLP is an e-mail scan of unencrypted e-mail traffic, to included attachments, to detect inappropriate transport of sensitive information, including sensitive information. in-transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Use of trusted internet connection (TIC)
- Anti-virus software to protect host/end-user systems
- HSPD-12 compliant PIV cards
- Access controls

The PSS systems also follow the National Institute of Standards and Technology (NIST) standards, including special publications 800-53, 800-63, and 800-37. Any system within the organization that contains, transmits or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. Finally, the organization also employs data loss prevention (DLP) solutions – the DLP is an e-mail scan of unencrypted e-mail traffic, to included attachments, to detect inappropriate transport of sensitive information, including sensitive information.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

__X__ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 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, number, and link. *(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, this system is not a system of records and a SORN is not applicable.

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: NARA GRS 5.6 – Item 010 (PACS Status/Badge Reports). Item 090 (CCTV)
	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	X
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

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. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

	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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: The system contains information which may directly identify unique individuals – either visually or by directly identifying information. 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. PACS contains employee's name and photograph.
X	Quantity of PII	Provide explanation: The system collects PII about a large number of individuals. CCTV system contains continuous video recording of internal and external HCHB cameras. PACS system contains records of all individuals who have authorized access to the HCHB.
X	Data Field Sensitivity	Provide explanation: Data included in the system includes that which is may be known to a small set of individuals, beyond the person to whom it pertains, on a need-to-know basis, but that, in and of itself may not lead to substantial harm, embarrassment, inconvenience or unfairness to the subject individual if compromised or otherwise inappropriately disclosed. CCTV data contains video and still images of both public and non-public spaces while the PACS system contains a combination of low and moderate sensitivity data.
X	Context of Use	Provide explanation: System contains records of individuals who have authorized access to the HCHB or who are in and around monitored spaces of 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 included in the PACS system – including data collected for the issuance of PIV cards and granting access to the HCHB and collected in accordance with the Privacy Act of 1974. DOC has an obligation to protect the confidentiality of CCTV data to ensure appropriate use in crime prevention, criminal prosecution, securing physical access, and for other reasons outlined in this PIA.
X	Access to and Location of PII	Provide explanation: : PII is maintained locally (within HCHB) with access limited only to internal, authorized DOC employees with a bona-fide need-to-know the information.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the

choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Use of the PSS, and the CCTV function, raises potential privacy risk related to notice, consent, and access. Each is discussed in further detail below.

There is a risk that individuals may be unaware that they are being recorded by CCTV cameras or may not understand why the recording is necessary.
This risk is mitigated in several ways. The first is the use of signs, posted in public areas in and around the HCHB, which read "Premises are under 24 hours recorded video surveillance" in large, clear print. These signs serve as notice that a particular area is being recorded by the DOC CCTV. DOC recognizes that some individuals may not see these signs or may not understand why video surveillance of their activities is occurring. DOC has published this PIA to provide further notice of its use of CCTV on and around HCHB premises.

There is a risk that individuals may not consent to being recorded by CCTV.
Visitors and employees in and or near the HCHB (and other Federal facilities for that matter) do not have a reasonable expectation of privacy – the use of CCTV is a Federal mandate within all Federal facilities and a common security practice within private, commercial, and federal spaces throughout the United States. No consent is required. However, DOC has posted signage to make individuals aware of its use of CCTV in and around the HCHB and have conducted and made this PIA available to provide notice.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: PACS: The information is collected from DOC federal employees, contractors, affiliates, guests and others as necessary via the United States Federal smart card for DOC Personal Identity Verification (PIV). The PIV card contains the necessary data for the cardholder to be granted access to Federal facilities, information systems, and assure appropriate levels of security for applicable DOC federal applications. 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.'
	No, the conduct of this PIA does not result in any required business process changes.

12.3 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.