Privacy Impact Assessment
for the

DHS CCTV Systems

DHS/ALL/PIA-042

July 18, 2012

Contact Point
Kevin Crouch
Chief of Staff
DHS Office of Security
(202) 447-5424

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) and its components deploy a number of Closed-Circuit Television (CCTV) systems throughout the department (See Appendix for detailed list). DHS' CCTV systems are used to obtain real-time and recorded visual information in and around federal worksites and facilities to aid in crime prevention and criminal prosecution, enhance officer safety, secure physical access, promote cost savings, and assist in terrorism investigation or terrorism prevention. DHS conducted this Privacy Impact Assessment (PIA) because these systems have the ability to capture images of people, license plates, and any other visual information within range of the cameras. This PIA replaces existing CCTV PIAs: those PIAs will be retired with the publication of this PIA and are listed in the appendix.

Overview

CCTVs are used for various reasons: to keep property safe and secure for federal employees; to provide a cost-effective method to monitor a location, provide archived video coverage for investigations; and to deter against future crime or attack.

DHS is responsible for the protection of federal facilities, employees, and visitors, which may be the target of acts of terrorism or other crimes such as robbery, burglary, or vandalism. Crimes in progress may be detected and possibly prevented since the video feeds can be monitored in real-time. Also, a clearly visible camera alerts the public that they are being monitored, which may deter criminal activity.

Networked security video systems typically consist of analog or IP cameras, recording devices, and monitoring capabilities with a network consisting of closed-circuit video cameras, video recorders, and monitoring capabilities that captures video-only feeds or a stand-alone system with one camera monitoring a specific area. The cameras are capable of streaming live video shots but most of the government networks of security video systems use firewalls to limit viewing to those in the viewing room or to those viewing through remote monitoring. The CCTV cameras include a series of fixed cameras and pan-tilt-zoom (PTZ)[1] cameras. The recording devices consist of Digital Video Recorders (DVRs) which use hard drives to store recorded video and Network Video Recorders (NVRs), which use mass storage devices with multiple arrays of hard drives. After the storage capacity is reached; the units automatically overwrite previously recorded video with the most recent images unless video has been identified to be retained for security purposes. This process is known as First In, First Out (FIFO). Regardless of storage capacity, DHS policy is to only retain video for six months.

Some cameras used for DHS CCTV systems utilize zoom capability with manual tracking (i.e., panning and tilting), which allows the officer conducting the monitoring to gain the best image of any activity. Other CCTV systems are set to automatically tour an area. The cameras are placed in various locations on the perimeters or inside of federal facilities, such as parking lots, entrances, and secured areas, to provide the greatest possible range and area of monitoring. Cameras contain low-light technology to support detection of unauthorized or suspicious activities at night. The cameras are not placed in areas with a reasonable expectation of privacy like bathrooms or changing rooms.

[1] PTZ means the camera can zoom in on both vertical and horizontal movement.

DHS uses the video feeds to detect and respond to potentially unlawful activities in real time in the areas using CCTV. The video feeds may also be used to support law enforcement investigations to the extent that they contain information relevant to a criminal (or potential criminal) activity. For example, if a suspicious package is placed outside a federal building that uses the system, the cameras will provide an image of this activity and allow DHS 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 suspects, and/or provide evidence that may be used in court.

DHS will use an image, such as a license plate number, captured by the video feed to identify an individual or link an individual to a specific event or investigation. In general, DHS will use CCTV feeds to further investigations, link data elements, and identify individuals.

Privacy protections for CCTV systems include limiting access to the video feed to only authorized users and law enforcement partners, establishing clear auditing systems so every use of the CCTV system is logged and reviewable and restricting storage to six months or less. Also, DHS users agree to a "Rules of Behavior" which subjects employees to administrative and potentially criminal penalties if any misuse occurs.

This PIA covers CCTV systems that only capture video; it does not cover the collection of audio. Some CCTV cameras used by DHS have audio capability but it is disabled for use. If audio is required for use, then a separate PIA will have to be completed.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

DHS has legal authority under 40 U.S.C. § 1315 to protect the buildings, grounds, and property owned, occupied, or secured by the federal government, and the persons on the property. In addition, the *Physical Security Criteria for Federal Facilities, An Interagency Security Committee Standard, Report* issued on April 12, 2010, and successor documents require CCTV monitors for the majority of federal buildings from low security requirements to very high.

The DHS Physical Security Construction and Equipment Handbook, May 27, 2010, requires CCTV for the protection of DHS Headquarters sites.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The SORNs for this PIA are DHS/ALL-024 - Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, February 3, 2010, 75 FR 5609,[2] and DHS/ALL-025 -

[2] http://edocket.access.gpo.gov/2010/2010-2206.htm.

Department of Homeland Security Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security, February 3, 2010, 75 FR 5614.[3]

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Each CCTV system should complete an individual system security plan unless the CCTV system is integrated into the other electronic security systems.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

DHS stores recorded video for six months after which the video is automatically deleted in accordance with National Archives and Records Administration (NARA) General Records Schedule (GRS) 21, Items 11 and 18 (routine surveillance motion picture and video recordings).

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Not applicable.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

DHS places the CCTV cameras around the perimeter and inside of DHS facilities and buildings, including parking lots, entrance and exits, and secured areas. The CCTV cameras may capture facial images of employees and visitors to DHS buildings and images of license plates that are parked or driving through the parking lot.

Additionally, some CCTV systems collect metadata. Metadata describes other data. It provides information about a certain item's content. For example, an image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data. A text document's metadata may contain information about how long the document is, who the author is, when the document was written, and a short summary of the document. Regarding a CCTV system, some examples are camera name, location, time, and date. The data is used to manage the CCTV feeds and footage files.

DHS uses the video feeds captured through CCTV to aid in crime prevention and criminal investigations, enhance officer safety, secure physical access, promote cost savings, and assist in terrorism investigation or terrorism prevention.

CCTV recordings may provide investigators with leads when investigating crimes occurring at

[3] http://www.gpo.gov/fdsys/pkg/FR-2010-02-03/html/2010-2207.htm

protected federal facilities. For example, CCTV records may assist investigators in identifying persons who were in the area when a crime occurred or identify suspects or vehicles fleeing the area. These videos may also become evidence in a subsequent criminal prosecution.

CCTV images can provide DHS personnel with real-time information on suspicious activities that may be related to terrorist activity, such as terrorist surveillance or actions in preparation for a terrorist attack. In addition, the CCTV recordings can be used for investigative and prosecutorial purposes in the event of an attack. DHS uses CCTV images to identify individuals and may try to identify individuals through other data elements like a license plate number captured by a CCTV feed.

Cameras are not placed in places with a reasonable expectation of privacy such as inside a bathroom or changing room.

If audio ability is incorporated and enabled into the CCTV system, then a separate PIA will have to be completed.

2.2 What are the sources of the information and how is the information collected for the project?

CCTV systems record video from a variety of ranges and with differing zooming capabilities. The cameras may record passersby on public streets and DHS employees accessing a secured area. 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 or text written on a person's belongings. 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. Tracking, which can be manual or occur when the cameras automatically track people or other moving objects in the field of view, is used so security personnel may follow the activity of a single individual within viewing areas that contain a large number of people.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Depending on the angle and zoom of the CCTV camera, video of an individual may be collected from a public space. Public areas surrounding federal facilities are monitored by CCTV systems. The video is used to render property safe and secure for federal employees, provide a cost-effective method to monitor a location, and deter against future crime or attack.

2.4 Discuss how accuracy of the data is ensured.

CCTV cameras collect real-time video of the activities occurring within their viewing space in or near federal buildings. The videos are altered through a compression algorithm in order to be stored in an array of hard drives but otherwise are not modified or changed to alter the recorded activities. CCTV

cameras only record what is occurring in real time; there is no editing feature or ability to change the image. Users can zoom or pan the cameras to follow one individual, but it is unlikely that incorrect information about a person is produced from the CCTV cameras.

Only authorized personnel have access to the stored video data, and all DHS employees must agree to a general "Rules of Behavior" before logging into any DHS system. The "Rules of Behavior" list the specific uses for the system and a notice that use of the system is audited through logs. The misuse of any system will subject employees to administrative and potentially criminal penalties. Additionally, all DHS CCTV systems will be password-protected, and access is restricted to only authorized users.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: The cameras will collect more information than is necessary to accomplish the purpose by the CCTV cameras.

Mitigation: This is mitigated by the placement of cameras in public places as opposed to bathrooms or other areas where individuals have a reasonable expectation of privacy. The purpose of the CCTV cameras is to protect the buildings, grounds, and property owned, occupied or secured by the federal government, and the persons on the property. CCTV cameras are only used to render property safe and secure for federal employees and deter against future crime or attack.

Privacy Risk: Video that is not relevant and necessary to accomplishing the mission will be collected and not recorded over.

Mitigation: DHS only uses the video feeds to detect and respond to potentially unlawful activities in real time or to support law enforcement investigations and prosecutions to the extent that they contain information relevant to a criminal (or potential criminal) activity. All other video feed is automatically overwritten once the storage capacity has reached its limit.

This is also mitigated by the "Rules of Behavior" users must sign and by administrative and potentially criminal penalties.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Information on the video is used by DHS and federal, state, and local law enforcement to detect and respond to potentially unlawful activities in real time in the areas surrounding federal facilities using DHS cameras. 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 that uses a DHS camera, the system would provide a real-time notification of this activity and allow DHS and federal, state, and 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.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

The DVR/NVR software is used to search for a specific video event or image.

3.3 Are there other components with assigned roles and responsibilities within the system?

DHS investigations unit, property crimes unit and security have access to the video but only after a supervisor approves dissemination.

Each CCTV system will have a policy in place outlining internal sharing including retention limits, access and what authority grants sharing.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: CCTV cameras may be used for improper surveillance or record more than is necessary.

Mitigation: The purpose behind DHS' use of a CCTV system is to detect and deter criminal activity, and to provide investigatory leads only. DHS cameras covered by this PIA do not record or transmit sound (i.e., audio).

Additionally, all DHS CCTV systems are password-protected, and access is restricted to only those who monitor the video feeds. The system tracks the users and will be periodically reviewed for misuse and discriminatory practices.

Finally, "Rules of Behavior" must be agreed to before any use of the system. The misuse of any system will subject employees to administrative and potentially criminal penalties.

Privacy Risk: Unauthorized access to a DHS system video feed may occur.

Mitigation: The risk is mitigated by the fact that the video feed is secured during transmission and only videos of stored data are available. Videos of stored data may only be released to those with law enforcement needs or in response to FOIA requests and DHS authorized personnel must grant permission for this release.

Users of any DHS system must read and sign a "Rules of Behavior" for use and operation of the system. The system itself limits the potential for misuse of the information on the video because it is not retained for a significant period of time. In addition, DHS personnel are subject to criminal and administrative penalties if they misuse the system for unauthorized purposes.

Privacy Risk: Use of CCTV cameras may restrict freedom of speech or association.

Mitigation: The system does not in any way restrict freedom of speech or association. The images are primarily used to detect and deter criminal activity. The images are not used to restrict or investigate lawful rallies and associations. The occurrence of First Amendment-protected activity, such as a protest or

rally outside a federal facility, is treated by DHS like any other activity that may be captured by a DHS camera. Unless there is evidence of criminal activity that must be investigated or prosecuted, DHS will not maintain those images for longer than the storage capacity of the DVR. DHS shares images only for legitimate law enforcement purposes or in response to FOIA requests.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

All DHS CCTV systems provide notice of the surveillance camera. Signs are posted in public areas, in written format or in pictograms. An example of the type of wording provided in such notice signs is:

"This Area Under Video Surveillance."

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals who enter or are near federal property do not have a reasonable expectation of privacy and therefore no consent is required. However, as a matter of policy, signs are posted to provide notice of surveillance activities via CCTV cameras.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Members of the public may not see the notice sign or may not be aware of why CCTV cameras are necessary.

Mitigation: The risk is mitigated by the publication of this PIA. This PIA makes clear that federal properties are under surveillance by CCTV cameras and why the cameras are necessary. Additionally, it has been a requirement since the 1995 Presidential Policy Memorandum for Executive Departments and Agencies titled *Upgrading Security at Federal Facilities* for federal facilities (where feasible) to install CCTV cameras. Federal buildings must be protected, and CCTV is a cost efficient and useful tool to prevent crime and terrorism. The use of CCTV is a common practice throughout the United States in the private, commercial, and federal arenas and is a standard security practice.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

Data is stored for a maximum of six months and then is automatically deleted.

Records which are retrieved pursuant to suspected criminal activity will be retained until any investigative or enforcement action is completed. To retain the footage after the retention period, a supervisor must approve the request and confirm the recordings are relevant to actual or suspected criminal activity.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that storing video for six months is too long.

Mitigation: The retention period is appropriately limited to only retain images for a short length of time, while still allowing DHS to identify potentially relevant video when a crime has occurred but is not immediately reported.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Local, state, and federal government agencies have access to several DHS CCTV systems (see appendix: Livewave). Additionally, individuals who were victims of a crime, criminal defendants, or members of the public through a Freedom of Information Act request may request copies of the video.

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.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Routine uses of records associated with visiting DHS facilities are addressed in; DHS/ALL – 024 Facility and Perimeter Access Control and Visitor Management, January 16, 2009, 74 FR 3081; and DHS/ALL-025 - Department of Homeland Security Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security February 3, 2010, 75 FR 5614.

6.3 Does the project place limitations on re-dissemination?

Consistent with the original collection, disclosure to federal, state, and local law enforcement agencies must be for terrorism and law enforcement purposes only.

Depending on the CCTV system the video can be shared through discrete portions of video footage or via hard copy.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Each individual CCTV system should maintain a record of all disclosures outside of the Department. This includes state, local, and federal law enforcement.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There may occur unauthorized or inappropriate sharing of CCTV images outside of DHS.

Mitigation: In most cases, external partners do not have real-time access to the video feeds. They may receive the video after it has been recorded which prevents inappropriate viewing of the public or specific locations by non-DHS users. External partners with access to DHS video feeds must follow specific memoranda of understanding or rules of behavior, as appropriate.

Requests for video must be approved by a supervisor and must be requested before the DVR overwrites the video. The DVR recordings are deleted by over-writing when the storage capacity is exceeded or within six months, whichever is shorter.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Individuals may access their information by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request to the DHS FOIA Office at 245 Murray Lane SW, Washington, D.C. 20528. Generally, CCTV Systems do not record or retrieve information by personal identifiers so it will be difficult for an individual to find and view a particular video. Additionally, videos are only stored for a maximum of six months and in some cases, a much shorter period of 30 days or less, depending on the age and condition of the equipment. The video is then recorded over, which limits the amount of time an individual has to access the video. Accordingly, an individual wishing to access their information should provide a detailed description, such as the address or physical location of the CCTV system, the date and approximate time the video or image was taken, or other identifying information that will assist DHS in locating the requested record.

For more information on specific procedures for submitting a FOIA/PA request, see http://www.dhs.gov/foia.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Video image cannot be corrected given it captures the events in real time, but an individual may complete a FOIA request to view the image. See the appendix for specifics on which department to contact.

7.3 How does the project notify individuals about the procedures for correcting their information?

This PIA serves to notify individuals about the procedures to correct their information. Consult the appendix for more specific details.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: The period of time for redress for an individual is very short. In most cases, video is not retained longer than six months.

Mitigation: Given the nature of CCTV systems, a robust program to permit access, review, and correction of the video cannot be provided. This lack of direct access and formal redress mechanism represent a risk to individual privacy; however it is necessary given the utility of CCTV systems and the retention rates. While some individuals will not have a formal mechanism for access or redress, DHS has internal mechanisms to correct inaccuracies and protect against abuse through the auditing system and the "Rules of Behavior" for users.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Only authorized users are allowed to view the video feeds of DHS CCTV systems. The log-in and use of the system is traceable to a particular user and periodically audited for misuse and discriminatory practices.

The system is audited when an employee with access leaves the organization or when called for by a supervisor. The audit is performed by someone within the organization but separate from the operational team.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

Training is provided to all DHS employees on handling of PII and correct uses of relevant systems. Training includes privacy, technical aspects of the system, and disciplinary procedures for violations. Training should also be extended to external and internal partners who may view the system in real-time.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Several security controls are in place to ensure unauthorized access does not occur including signal encryption and password protection.

Only authorized users are allowed to view the video feeds of DHS CCTV systems. The log-in and use of the system is traceable to a particular user and periodically audited for misuse and discriminatory practices. The DVRs themselves are also physically protected against unauthorized access.

Finally, "Rules of Behavior" must be agreed to and signed before any use of the system. The misuse of any system will subject employees to administrative and potentially criminal penalties. Additionally, an internal policy must be in place detailing access rules and violations, including any internal or external partners.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

DHS has formal and informal agreements with state, local and federal government agencies granting access to CCTV systems. The purpose behind these agreements is to share information if cross-jurisdictional law enforcement is needed, i.e., if the local police department has to investigate criminal activity that occurred or is occurring in the proximity of the federal building, and to perform night time perimeter viewing for safety and security reasons.

These agreements should discuss: usage, retention period, access, dissemination and security of the system. DHS Component Privacy Offices will periodically audit these agreements to ensure accuracy and compliance.

Responsible Officials

Kevin Crouch
Office of Security
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix

PIAs

Livewave CCTV System (DHS/NPPD/PIA-012, September 17, 2009)

The Livewave Closed-Circuit Television (CCTV) system is owned and operated by the Federal Protective Service (FPS), an operational component within National Protection and Programs Directorate (NPPD). The Livewave CCTV system is a video-only recording system installed in several secure federal facilities in New England. Livewave is similar to other FPS CCTV surveillance systems in secure federal buildings with the exception that it can be viewed and controlled remotely over an Internet connection, whereas other FPS CCTV systems are monitored on site. Remote viewing allows FPS to maximize staffing resources by centralizing system monitoring.

In addition to the requirements listed in this PIA, the Livewave CCTV System follows the following guidelines:

- Livewave can be viewed and controlled remotely over an internet connection allowing for remote viewing of real time images.
- The Boston Massachusetts Police Department has been provided access to the external Livewave CCTV feed for one federal building in Boston but does not have access to the DVR or the ability to control the tracking features on the camera.
- External partners are required to read and sign the "Rules of Behavior."
- The retention period for video footage is a maximum of one month unless the video contains information that is relevant to actual or suspected criminal authority.

Nebraska Avenue Complex CCTV System (DHS/ALL/PIA-035, March 2, 2011)

The Department of Homeland Security (DHS), Office of the Chief Security Officer (OCSO), Physical Access Security Division (PHYSD) operates the Physical Access Control System (PACS). PACS is designed to coordinate access control, intrusion detection, and video surveillance at DHS Headquarters (HQ) facilities in the National Capital Region (NCR), primarily the Nebraska Avenue Complex (NAC). The purpose of the system is to enable OCSO PHYSD and its Force Protection Branch (FPB) personnel, including security guards, the ability to obtain current state visual information as well as information on or related to a security-related incident that is happening or has happened and to deter criminal activities.

In addition to the requirements listed in this PIA, the NAC CCTV System follows the following guidelines:

- There is no external sharing of images captured by the NAC CCTV System outside of DHS.

The SORN for this PIA is DHS/ALL-024 – Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, February 3, 2010, 75 FR 5609 (http://edocket.access.gpo.gov/2010/2010-2206.htm).

Security Management CCTV System (DHS/ICE/PIA-030, August 4, 2011)

The Security Management Closed-Circuit Television System (SM-CCTV System) is owned and operated by U.S. Immigration and Customs Enforcement (ICE). The SM-CCTV System is a video-only recording system installed to monitor the interior and exterior of ICE facilities.

In addition to the requirements listed in this PIA, the Security Management CCTV System follows the following guidelines:

- A camera is located in the security command center to monitor the room and what is being viewed on the monitors.
- Auditing of the system occurs once a week.

PTAs

- NPPD FPS Region 2 CCTV

FPS provides law enforcement and protective security services under Title 40 United States Code, Section 1315, for Federal facilities that have in place closed circuit television cameras (CCTVs) that provide real time, continuous video of the public spaces in, on, and adjoining these Federal facilities. In FPS Region 2, FPS and the New York Police Department (NYPD) realize the critical need for data sharing and cooperation for public safety and law enforcement purposes and will work as partners to enhance the safety and security of the people who live and work in Manhattan. Inasmuch as FPS Region 2 has Facility Security Level IV[4] buildings in this area, FPS has sought to leverage the NYPD's extensive, existing network of countermeasures to augment the security of those Federal facilities protected by FPS. Toward that end, FPS has entered into a formal Memorandum of Understanding (MOU) with the NYPD that incorporates the following key elements:

[4] On March, 10, 2008, the Interagency Security Committee issued new standards for determining the security level of Federal facilities that supersede the standards developed in the Department of Justice's 1995 Vulnerability Assessment Guidelines. These guidelines have five security levels. A level IV facility has over 450 employees, a high volume of public contact, and includes high-risk law enforcement and intelligence agencies.

- FPS will share its CCTV feeds with NYPD (all camera views will be of public space; includes metadata).
- NYPD may retain and archive video from FPS CCTV feeds for up to 30 days.
- FPS will have a full-time seat at the Lower Manhattan Security Coordination Center during business hours to view data collected from all of the FPS locations and for security briefings. (January 4, 2012.)

- US-VISIT CCTV

US-VISIT is installing closed circuit television's (CCTV) in the publicly-accessible lobbies of its 3 office locations: 1) 1616 Fort Myer Drive, Arlington, VA; 2) 1550 Wilson Drive, Arlington, VA; 3) 9275 Sky Park Drive, San Diego, CA. Additionally, US-VISIT is installing camera-capable ceiling tiles that will not actually record or contain cameras but will give the effect that it is. The purpose of these efforts is to prevent and deter crime and unauthorized access into the DHS facilities by monitoring the access-controlled entryways from the lobbies and creating the effect of monitoring inside workspaces. (January 23, 2012.)

- NPPD CCTV

NPPD installed a CCTV system to monitor and record the exterior entry and exit points of DHS-controlled areas on the 6th and 19th floors of 1616 Fort Myer Drive, Arlington, Virginia. The purpose of the system is to deter theft and to provide evidence of suspected crimes and other unauthorized activities. (April 2, 2012.)

- USSS HELIX

USSS HELIX, formerly operating as CROWN CCTV P3C is a USSS security surveillance system that supports law enforcement and protective security. The surveillance system consists of security video cameras, video storage arrays, and video management systems (VMS) that capture live video feeds of spaces in, around, and adjoining to locations that are permanent and/or temporarily under the protection responsibility of the USSS. The purpose of the system is to provide situational awareness for the protective mission, to utilize a cost-effective method to monitor protective locations, to document matters related to national security and legitimate law enforcement purposes, to enhance law enforcement officer safety, and to provide a potential deterrent to criminal activity and/or terrorist attack. The cameras utilized in USSS surveillance systems include both fixed view and pan-tilt-zoom (PTZ) capabilities. The video captured by the surveillance systems reside on storage arrays housed in Government controlled and managed equipment. That equipment is only accessible to USSS authorized personnel. Each system contains enough storage capacity to retain all recorded surveillance video for 30 days, after which the data is overwritten, pursuant to NARA DAA-0087-2014-0001 data retention policies. (October 4, 2023.)

- USSS Video and Alarm Platform

USSS Video and Alarm Platform is a USSS security surveillance system that supports law enforcement and protective security. The surveillance system consists of security video cameras, video storage arrays, and video management systems (VMS) that capture live video feeds of spaces in, around, and adjoining to locations that are temporarily under the protection responsibility of the USSS. The purpose of the system is to provide situational awareness for the protective mission, to utilize a cost-effective method to monitor protective locations, to document matters related to national security and legitimate law enforcement purposes, to enhance law enforcement officer safety, and to provide a potential deterrent to criminal activity and/or terrorist attack. The cameras utilized in USSS surveillance systems include both fixed view and pan-tilt-zoom (PTZ) capabilities. The video captured by the surveillance systems resides on storage arrays housed in government controlled and managed equipment. That equipment is only accessible to USSS authorized personnel. Each system contains enough storage capacity to retain all recorded surveillance video for 30 days, after which the data is overwritten, pursuant to NARA DAA-0087-2014-0001 data retention policies. (February 23, 2024.)

- PIADC FSS

Plum Island Animal Disease Center (PIADC) is a federally owned and operated facility that conducts animal and biological research for DHS. PIADC is implementing an updated comprehensive facility security system that will include an Electronic Entry Control System (EECS), an Intrusion Detection System (IDS), and a CCTV Surveillance and Assessment System. The CCTV Surveillance and Assessment System will include Digital Video Recorders (DVRs). The static range and zoom range vary, and tracking is done manually. This system uses real-time monitoring to record individuals entering federal facilities. The retention period for video footage is 30 days, and the footage is automatically deleted after the retention period expires. (May 7, 2013.)

- FPS WMATA MOU

FPS and the Washington Metropolitan Area Transit Authority (WMATA), Metro Transit Police (MTP) Department realize the critical need for data sharing and cooperation for public safety and law enforcement purposes and will work as partners to enhance the safety and security of the people who live and work in the National Capitol Region. As such, WMATA/MTP is adding FPS as a party to an agreement that will allow FPS access to WMATA/MTP Internet Protocol (IP) cameras at metrorail entrances. WMATA/MTP will share its live CCTV feeds with FPS (all cameras are located at Metro stations throughout NCR) during law enforcement incidents occurring on or near Metro stations. FPS will not retain or share the live video portion of any camera feed or release the location of any camera; nor will FPS manipulate the camera feeds, such as by selecting cameras, camera angles or zoom. (January 8, 2014.)

- CBP Block 1

Block 1 is part of the Border Surveillance Systems (BSS), which is an integrated technology solution to provide enhanced detection, tracking, response, and situational awareness capabilities along the U.S. border. Block 1 system combines day/night cameras with sensors and radar to assist front-line CBP personnel to effectively deter, detect, and resolve illegal cross-border activity along Arizona - Mexico border.

A key part of the Block 1 technology program is the Command and Control (C2) Common Operating Picture (COP), which provides Border Patrol agents the ability to monitor the border with real-time situational awareness of their area of responsibility and act as a force multiplier, allowing fewer agents to cover more ground. (July 15, 2014.)

- CG PACS

The U.S. Coast Guard (USCG) Physical Access Control Systems (CG PACS) encompasses multiple processes and electronic system nodes and applications in order to support: Physical Access Control to all Coast Guard facilities or units or portions thereof; identity verification for all employees, contractors, service providers and visitors; movement monitoring and security camera monitoring and recording of persons, vehicles, buildings, grounds and portions thereof, and Intrusion Detection Systems (IDS) operations.

To support physical access control for all USCG facilities, the Coast Guard may install CCTV cameras to monitor USCG Entry Control Points (ECP) and associated traffic lanes, police or guard facilities and houses, weapons ranges, critical infrastructure (power distribution facilities and components, generators, fuel storage, weapons armories and storage, ammunition and pyrotechnics storage, pumping stations, piers, boat ramps, storage facilities and yards, airfields and hangars, information technology facilities/buildings/rooms, antenna fields), building entrances/exits and stairwells, classified material storage and workspaces, walkways, roadways and parking areas in high crime areas and elevators.

- Transportation Security Laboratory (TSL) Video Camera Management System (VCMS)

DHS Science and Technology (S&T) TSL uses a physical security package to protect and secure TSL personnel, facilities, vehicles, and building environmental systems. One system in that package is the VCMS. The VCMS is a CCTV system.

TSL maintains video surveillance of the TSL campus. The VCMS controls and selects which cameras are shown on the monitors viewed by facility guard(s). Account name and password are required for a user to be granted access to the system. No specific names, other than the account holders to the computer, are stored on the VCMS computer. TSL maintains a highly restrictive physical access posture. Only authorized individuals are permitted within the controlled perimeter of the TSL. This limits the number of recognizable, authorized individuals operating within the laboratory perimeter and enables the guard force to more easily identify unauthorized

individuals. The cameras are motion-sensed to turn on and off depending on movement in facility. The video footage is stored on the computer for a minimum of 30 days, with the possibility of up to 90 days depending upon the level of activity within the area. After the pre-determined storage period the data is overwritten. The TSL VCMS only cover the grounds of the TSL. At the main entrance, there are signs that state "Security Notice, Video Surveillance in Use on these Premises." (August 28, 2018)

- Federal Emergency Management Agency

FEMA deploys a number of Closed Circuit Television (CCTV) systems throughout the agency in support of its Physical Access Control System (PACS) functions. FEMA's CCTV systems are used to obtain real-time and recorded visual information in and around its federal worksites and facilities to aid in crime prevention and criminal prosecution, enhance officer safety, secure physical access, promote cost savings, and assist in terrorism investigation or terrorism prevention. These systems have the ability to capture images of people, license plates, and any other visual information within range of the cameras. FEMA's CCTV system capability may be used when necessary to protect the health and/or safety of the individuals within the facility. FEMA's video surveillance function is further discussed in its PACS PIA: DHS/FEMA/PIA-051 Physical Access Control System.

- Transportation Security Administration (TSA) Office of Security Network (OSN)

TSA Office of Security Network (OSN) is an enterprise, integrated physical security management system providing card access/entry control, visitor management and integrated video imaging/badging in conjunction with security alarm monitoring and control (intrusion detection), and CCTV alarm call-up in a single system platform. OSN CCTV is used for alarm detection and response, to identify individuals, link data elements and to further investigations. TSA further discusses how it manages visitors to TSA facilities in its PIA for DHS/TSA/PIA-004 Visitor Management System (VMS).

- USCG Shipboard Closed-Circuit Television (CCTV)

The Shipboard Closed-Circuit Television (CCTV) is a system that provides live recorded video monitoring of shipboard systems. The Shipboard CCTV surveillance cameras' purpose is to provide 24/7 real time monitoring of all major engineering and auxiliary spaces. If the video needs to be retrieved as evidence for a flight deck mishap or law enforcement case, it can only be downloaded via an encrypted hard drive connected to the Digital Video Recorder Universal Serial Bus port or from the Digital Video Recorder (DVR) Digital Versatile Disc Drive by an authorized user. Any video recordings not used as evidence for a flight deck mishap or law enforcement case are only retained for 30 days on the Digital Video Recorder and then automatically overwritten.

While Shipboard CCTV may inadvertently capture faces of individuals, it is not used in conjunction with a facial recognition system or the collection of personally identifiable information. (November 30, 2023)

- USCG Waterways Commerce Cutter Acquisition (WCC) – Video System

The Waterways Commerce Cutter Video system includes the sub-systems and components necessary to provide Topside Surveillance (3TV), Interior Surveillance (14TV), and the Electro-Optical Surveillance System functionality, which is used to monitor activity of vital equipment, such as control panels, switchboards, compartments, passageways, working spaces, and operating spaces, and the exterior environment. All three sub-systems create video data (without audio) and metadata, such as the camera identification, field of view information, time stamp, system status, and ship position. This information is stored within the Waterways Commerce Cutter's Video System for no more than 30 days in accordance with the approved USCG Record Schedule. The Waterways Commerce Cutter's Video system enables the distribution and playback of live and recorded video throughout the ship, which cannot be transferred outside of the system except via manual means using writeable media. The video distribution components also support the distribution of data from the integrated satellite television reception system and other entertainment media. While Waterways Commerce Cutter Video system may inadvertently capture faces of individuals, it is not used in conjunction with a facial recognition system or the collection of personally identifiable information. (November 30, 2023)

- USCG Marine Transportation Cutter-Heavy (MTC-H) Video System

The Marine Transportation Cutter-Heavy Video System includes the sub-systems and components necessary to provide Topside Surveillance (3TV), Interior Surveillance (14TV), and the Electro-Optical Surveillance System functionality, which is used to monitor activity of vital equipment, such as control panels, switchboards, compartments, passageways, working spaces, and operating spaces, and the exterior environment. All three sub-systems create video data (without audio) and metadata, such as the camera identification, field of view information, time stamp, system status, and ship position, all of which are stored within the Marine Transportation Cutter-Heavy Video System for no more than 30 days in accordance with the USCG Record Schedule. This system enables the distribution and playback of live and recorded video throughout the ship, which cannot be transferred outside of the system except via manual means using writeable media. The video distribution components also support the distribution of data from the integrated satellite television reception system and other entertainment media. Additionally, the Marine Transportation Cutter-Heavy Video system is incapable of performing any digital signal processing, such as facial recognition, and is not intended to specifically capture facial images, nor is it deployed at head-height to specifically capture full, forward-facing facial features, though it

may inadvertently capture such details as personnel moving within view of the cameras. The Marine Transportation Cutter-Heavy Video system does not store or process personally identifiable information. (November 30, 2023)

- Cutter Video Recording System (CVRS)

The Cutter Video Recording System (CVRS) is a system that records directly from a Cutter's flight deck video system cameras and from Electro Optic and Infrared (EO/IR) cameras that records operations such as at-sea boardings, Search and Rescue (SAR) missions, helicopter operations, and images of personnel and others, including refugees and asylees that may have been interdicted. CVRS records the ability to recognize an image as a person, but are not detailed enough to make identification of specific individuals using facial recognition. The settings of the cameras, and Digital Video Recorder that captures the images, do not permit facial images large enough and with enough resolution detail (adequate number of pixels) to recognize a specific individual. CVRS is installed on 87' patrol boats and Medium Endurance Cutters, and are directly connected to the EO/IR cameras and flight deck video system cameras.

The video is recorded onto a dedicated Commercial Off the Shelf (COTS) Digital Video Recorder (DVR), which is not connected to any other network or system. If the video needs to be retrieved as evidence for a flight deck mishap or law enforcement case, it can only be downloaded via an encrypted hard drive connected to the Digital Video Recorder Universal Serial Bus port or from the DVR Digital Versatile Disc Drive by an authorized user. The video recordings are retained for 30 days on the DVR and then automatically overwritten. CVRS is not used in conjunction with a facial recognition system. In addition, personnel recorded during flight deck operations are required to wear Personal Protective Equipment (PPE) (e.g., helmets, goggles). Facial recognition software would not be able to make positive identification of a video image of an individual wearing PPE. Likewise, the IR video images recorded from the EO/IR cameras couldn't be used by any facial recognition software to make positive identification. The video recordings are retained for 30 days on the DVR and then automatically overwritten to ensure disposal. If records are retained due to a flight deck mishap or law enforcement case, those recordings would follow the requisite records retention schedule. (March 7, 2024.)

- Offshore Patrol Cutter (OPC) Video System (VS)

The Offshore Patrol Cutter (OPC) Video System (VS) consolidates surveillance camera video, sensor video, and off-ship video sources into a common video recording and distribution system. These video sources will record at-sea boardings, deck operations, small boat launch and recovery, helicopter operations, interdictions, and embarking and disembarking images of personnel to include refugees and asylees, as well as activities outside and inside the cutter. The video system

will capture streaming video of shipboard operations (internal and external) that includes images of personnel. The system will not be used in conjunction with a facial recognition system; however, classified spaces will have external cameras focused on the entry to the spaces, and facial images will be used to verify the identity of a person requesting entry to classified spaces. The identity of facial images are not involved in cross referencing of any other databases. The facial images will be verified by sight recognition only by the cutter crewmember inside the classified space prior to entry. The facial images may also be used at a later time to view persons who have accessed classified spaces.

Video recordings of these operations may be used to support law enforcement, physical security, and cutter training. The recording and distribution system uses Internet Protocol (IP) networking for distributing the video from sources (e.g., cameras, sensors) to workstation and entertainment displays. These requirements are Offshore Patrol Cutter Operational Requirements Document (ORD) 2.0, System Work Breakdown Structure (SWIBS) 439. The images will be destroyed at three years in accordance with NARA's retention schedule N1-026-05-07. (March 7, 2024.)

- FLETC Enterprise Security System (ESS) Video Surveillance System

FLETC uses the Enterprise Security System (ESS) to standardize the process for students, contractors, visitors, and personnel to obtain access to FLETC facilities. ESS includes its own Video Surveillance System, IP cameras including other required hardware, software, and storage integration at each FLETC location. The system will provide situational awareness at access points and critical infrastructure to assist unauthorized access detection via strategically located cameras. The only stored data is the video footage which is stored on a secured drive in the IT Server room at each FLETC site. No other data is collected or stored by the system.