Privacy Impact Assessment
for the

Security Management CCTV System

August 4, 2011

DHS/ICE/PIA-030

Contact Point
Timothy Moynihan
Assistant Director, Office of Professional Responsibility
U.S. Immigration and Customs Enforcement
(202) 732-8300

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

Abstract

The Security Management Closed-Circuit Television System (SM-CCTV System) is owned and operated by U.S. Immigration and Customs Enforcement (ICE), a component agency within the Department of Homeland Security (DHS). The SM-CCTV System is a video-only recording system installed to monitor the interior and exterior of ICE facilities. ICE conducted this Privacy Impact Assessment (PIA) because the system has the ability to capture images of people, license plates, and any other visual information within range of its cameras.

Overview

The SM-CCTV System is a computer network consisting of closed-circuit video cameras, digital video recorders (DVRs), and monitoring capabilities that capture video-only feeds in and around ICE facilities. The purpose of the SM-CCTV System is to help ICE secure and regulate physical access to ICE facilities. The system also serves to enhance officer safety, prevent crimes, and assist in the investigation of criminal acts committed inside and on the perimeter of protected ICE facilities. Video surveillance also supports terrorism prevention and facility protection with its visible presence, and detects and deters unauthorized intrusion at ICE facilities. The SM-CCTV System is planned to be deployed in numerous ICE facilities nationwide.

ICE's Office of Professional Responsibility (OPR), Security Management Unit (SMU) operates the Security Management System (SMS), of which the SM-CCTV System is one component, in support of its mission to protect ICE facilities across the United States. SMS is designed to coordinate access control, intrusion detection, and video surveillance at ICE facilities. In addition to the SM-CCTV System, SMS includes two other components: one for visitor management and another for physical access control and physical intrusion detection. This PIA only addresses the video surveillance portion of SMS: the SM-CCTV System. The remaining components of SMS are covered by the DHS Physical Access Control System PIA.[1]

ICE facilities are protected by Protective Security Officers (PSOs) provided by the Federal Protective Service (FPS). FPS is an operational component within DHS that provides law enforcement and security services to more than 8,800 Federal facilities nationwide. PSOs are contractors hired by FPS to provide law enforcement and security services.

Background

On April 19, 1995, the day after the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, the President directed the Department of Justice to conduct a vulnerability assessment of federal buildings in the United States, particularly their vulnerability to acts of

[1] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Physical Access Control System* (Jun. 9, 2011), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_pacs.pdf.

terrorism and violence. On June 28, 1995, the Department of Justice and the U.S. Marshals Service issued a report called "Vulnerability Assessment of Federal Facilities," which included recommended minimum standards for securing federal facilities. The report concluded that all federal facilities should use CCTV systems with at least time-lapse recording. Video recordings were determined to be valuable for deterrence, investigative, and evidentiary purposes. The report also recommended the posting of signs providing notice that the video surveillance was taking place to serve as a deterrent. The SM-CCTV System was installed according to these recommendations.

SM-CCTV System

The SM-CCTV System captures video of the general public on the exterior and interior of some ICE facilities with plans to roll out the SM-CCTV System to all ICE facilities. The SM-CCTV System cameras also capture video of ICE federal and contractor employees, and visitors to ICE facilities. Cameras are used within and on exterior perimeters of ICE facilities and are placed to observe egress/ingress routes into ICE facilities. Cameras are also placed to observe traffic in hallways and rooms that are considered sensitive to the operations of ICE. The SM-CCTV System consists of both fixed and pan-tilt-zoom cameras with 30x zoom lenses. Each ICE facility with SM-CCTV System equipment has its own recording devices consisting of digital video recorders (DVRs). The DVRs store approximately 180 days of video and overwrite previously recorded video with the most recent images upon reaching storage capacity.[2] The chronological nature of this video recording prevents DHS from retrieving video information by the name of an individual or some identifying number, symbol, or other particular assigned to the individual. The SM-CCTV System does not record or transmit sound (i.e., audio). The SM-CCTV System and other SMS components reside on the ICE network. However, SM-CCTV video traffic does not travel over the ICE network but is restricted to storage at each location that utilizes the SM-CCTV System.

OPR/SMU personnel and Protective Security Officers (PSOs) use the SM-CCTV System and other SMS components. In the system, these users are categorized as either: (1) Operators or (2) System Administrators. Operators of the SM-CCTV System consist of both OPR/SMU personnel and PSOs. Operators have the ability to view live and recorded video from the facility at which they are located. The SM-CCTV System prevents Operators from saving copies of video. All System Administrators of the SM-CCTV System, comprised solely of OPR/SMU personnel, have the capability to copy video from the DVRs to portable electronic media. Only System Administrators who are OPR/SMU supervisors are authorized to delete video, and deletion occurs at the DVR itself.

[2] Exact storage capacity will vary depending upon the frame rate, resolution, image quality, the average amount of movement in the scene, along with the number of cameras and DVRs at the facility. Typically there is between 90 to 180 days of storage capability.

Access to video through the SM-CCTV System is restricted to each specific facility and video from a specific off-site location may only be viewed after the video has been exported from the SM-CCTV System to portable electronic media. Authorized users of the SM-CCTV System will be able to access the system and/or view video in one of two ways: (1) through an SMS workstation located at ICE facilities or (2) by viewing live video displays at certain guard posts or offices at ICE facilities. A SMS workstation is a computer terminal on which SMS software has been installed to allow it to logon to the SM-CCTV system and view other SMS component systems. Cameras with pan/tilt/zoom capabilities may be controlled using a joystick and keyboard attached to SMS workstations. SMS workstations in the facility may be located in individual office areas or in a security command center staffed by OPR/SMU personnel and PSOs. A security command center allows OPR/SMU personnel and PSOs to monitor real-time and recorded video using multiple SMS workstations and display screens located in the center.

In addition, at certain facility guard stations and offices, ICE video displays may show live video feeds from nearby cameras via a hard wire connection and not an SMS workstation. These video displays only show live video feeds; recorded video is not available, the cameras do not have pan/tilt/zoom capabilities, and video may not be saved to external electronic media. As with SMS workstations, authorized personnel at these guard stations and offices may only view video from the ICE facility at which they are located.

SM-CCTV System video feed at ICE facilities is continuously monitored by PSOs and OPR/SMU personnel. If suspicious activity is observed, PSOs or OPR/SMU personnel are dispatched to the scene to investigate. Relevant video may then be saved to DVD in the event it is needed for further investigation of the incident. Video saved to portable electronic media is used to support criminal, terrorism, or internal disciplinary investigations. The retention period for saved video depends on its use and is likely to vary by the type of investigation or inquiry for which it is being saved.

Section 1.0 The System and the Information Collected and Stored Within the System

The following questions are intended to define the scope of the information collected, as well as the reasons for its collection as part of the program being developed.

1.1 What information is to be collected?

(Please check the following if applicable)
The System's Technology Enables It to Record:

☒ Video
Static Range: 30ft
Zoom Range: 1000ft
☒ Tracking

☐ Automatic (for example, triggered by certain movements, indicators)
☒ Manual (controlled by a human operator)

☐ Sound
Frequency Range:

The System Typically Records:

☒ Passersby on public streets.
☒ Textual information (such as license plate numbers, street and business names, or text written on recorded persons' belongings).
☒ Images not ordinarily available to a police officer on the street:
☒ Inside commercial buildings, private homes, etc.
☒ Above the ground floor of buildings, private homes, etc.

Cameras are placed inside of ICE facilities to observe traffic in hallways and rooms that are considered sensitive to the operations of ICE. In addition, cameras are used within and on exterior perimeters of ICE facilities and are placed to observe egress/ingress routes into ICE facilities. This includes cameras placed above the ground floor on buildings to view a larger area surrounding the building.

1.2 From whom is the information collected?

☒ General public in the monitored areas.
☐ Targeted populations, areas, or activities (please describe).
☐ Training included directives for program officials to focus on particular people, activities, or places (please describe).

1.2.1 Describe any training or guidance given to program officials that directs them to focus on particular people, activities, or places.

There is no training or guidance given to system users directing them to focus on particular people, activities, or places. Those monitoring the system use common sense, on-the-job experiences, and experiences gained from working with other personnel in the security command center in order to properly identify potentially criminal or suspicious activities and use SM-CCTV System cameras' zoom and panning capabilities to manually focus on those activities.

1.3 Why is the information being collected?

☒ Crime prevention
☒ To aid in criminal prosecution
☐ For traffic-control purposes
☒ Terrorism investigation

☒ Terrorism prevention
☒ Other (please specify): To assist DHS in securing and regulating physical access to ICE facilities.

1.3.1 Policy Rationale

☒ A statement of why surveillance cameras are necessary to the program and to the governmental entity's mission.

ICE facilities, employees and visitors, which may be the target of acts of terrorism or other crimes such as robbery, burglary, or vandalism. The cameras serve as a means to detect and deter these acts, and also as a force multiplier insofar as one individual may monitor many exterior and interior areas of an ICE facility from one location at the same time. This also provides a cost savings since fewer personnel are needed to secure the facility.

☒ Crime prevention rationale: (for example, crimes in-progress may only be prevented if the cameras are monitored in real-time. Or, a clearly visible camera alerting the public that they are monitored may deter criminal activity, at least in the monitored area.)

The SM-CCTV System helps to detect and prevent unauthorized entry into ICE facilities and other crimes in progress because of both the visible presence of the cameras and the fact that video feeds are monitored in real-time. Also, clearly visible cameras and posted signs indicating that individuals are subject to video surveillance alert the public, employees, and visitors to the fact that they are being monitored, which may deter criminal activity.

☒ Crime investigation rationale: (for example, a hidden camera may be investigative but not preventative, providing after-the-fact subpoena-able records of persons and locations.)

Recordings from the SM-CCTV System may provide investigators with evidence of crimes occurring at ICE facilities, could also provide leads for investigators to follow in investigating crimes, and could become evidence in potential criminal prosecutions. For example, video records may identify persons who were in the area when a crime occurred, or identify suspects or vehicles fleeing the area.

☒ Terrorism rationale: (for example, video footage is collected to compare to terrorist watch lists.)

Images captured by the SM-CCTV System can provide 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 on an ICE facility. The images can also be used for investigative and prosecutorial purposes in the event of an attack.

1.3.1.1 Detail why the particular cameras, their specific placement, the exact monitoring system and its technological features are necessary to advance the governmental entity's mission. For example, describe how low-light technology was selected to combat crime at night. It is not sufficient to merely state the general purpose of the system.

Cameras are placed in elevated locations on the perimeters of the ICE facilities to provide the greatest possible range and area of surveillance; this allows the personnel monitoring the video feed to have the greatest situational awareness and visibility into activities occurring outside the buildings. Cameras are placed within ICE facilities to monitor specific entry and exit points to areas of interest within the facility, such as the loading dock, the parking garage, and hallways in the building interiors, where unauthorized entry or exit may be attempted by persons seeking to do harm. Cameras used for this system contain low-light technology to support detection of unauthorized or suspicious activities at night. The cameras also use pan/tilt/zoom capability with manual tracking, which allows the individual conducting the surveillance to adjust the camera in real time to gain the best image of any suspicious or illegal activity of interest that is occurring. Manual tracking was chosen so that the security personnel may follow the activity of a single individual within viewing areas that contain a large number of people. Automatic tracking would fail in this scenario.

1.3.1.2 It would be adequately specific, for example, to state that cameras which are not routinely monitored provide after-the-fact evidence in criminal investigations by providing subpoenable records of persons and locations. Similarly, it would appropriate to state, for example, that video footage is collected to compare to terrorist watch lists and wanted persons lists.

Video recordings may be used to gather investigatory evidence pertaining to suspected criminal activity or provide evidence for the prosecution of crimes that take place in or around ICE facilities. The output from all video cameras is recorded on the DVR, regardless of whether that specific camera is currently being monitored or manually operated by PSOs or OPR/SMU personnel. As such, even the cameras which are not being monitored or manually operated may provide after the fact evidence in criminal investigations by providing subpoenable records of persons.

1.3.1.3 How is the surveillance system's performance evaluated? How does the government assess whether the surveillance system is assisting it in achieving stated mission? Are there specific metrics established for evaluation? Is there a specific timeline for evaluation?

The system is primarily a prevention and deterrent system. It is difficult to measure what crimes were prevented by the system, because they did not occur. However, the system does

help to monitor large perimeter areas that PSOs and OPR/SMU personnel cannot necessarily patrol at all times, and as such, it increases the effectiveness of physical security controls. The system also provides cost savings by reducing the number of personnel needed to provide the same level of physical security by allowing fewer employees to monitor large areas. The system is not currently evaluated on a regular basis using specific metrics or timelines because, as stated above, it is largely a preventative and deterrent system.

1.3.2 Cost Comparison

Please describe the cost comparison of the surveillance system to alternative means of addressing the system's purposes.

The cameras provide a force protection insofar as one individual may monitor many exterior areas from one location at the same time. This also provides a cost savings since fewer personnel are needed to secure the facility. It is difficult to provide an exact cost savings. There is a cost savings by using video cameras to replace personnel who might patrol a given area, as analog video cameras and pan/tilt/zoom low-light cameras are far less expensive than the cost of full time workers for the same duration.

1.3.3 Effectiveness

☐ Program includes evaluation of systems performance (please describe how performance is evaluated.)
☐ Evaluation includes metrics to measure success (for example, crime statistics.)
☐ Program includes a timeline for evaluation

ICE does not employ any standardized means for evaluating the effectiveness of the system because the system is largely a preventative and deterrent tool.

1.4 How is the information collected?

☐ Real-time monitoring, with footage streamed, but not stored.
☒ Real-time monitoring with footage stored.
☐ Footage not monitored, only stored.

1.4.1 Describe the policies governing how the records can be deleted, altered or enhanced, either before or after storage. Are there access control policies limiting who can see and use the video images and for what purposes? Are there auditing mechanisms to monitor who accesses the records, and to track their uses, and if so, are these mechanisms a permanent and unalterable part of the entire system? What training was conducted for officials monitoring or accessing the technology?

Describe the policies governing how the records can be deleted, altered or enhanced, either before or after storage.

The information is collected in real-time by the cameras and stored on DVRs. The DVR recordings are deleted by over-writing when storage capacity is exceeded, approximately every 90-180 days. Over-written video is lost unless it has been saved to portable electronic media. Video may be saved to portable electronic media where suspicious activity is observed or when it is required to document an event or incident. The Assistant Director/OPR, Division Director/OPR/Security, or Deputy Division Director/OPR/SMU must provide prior approval for video to be saved from the DVR to portable electronic media. The investigating officer requests this approval via email and the request and approval are kept in the ICE Physical Security Outlook file manager. Once the Assistant Director/OPR, Division Director/OPR/Security, or Deputy Division Director/OPR/SMU's approval is provided, a System Administrator saves the video to the preferred portable electronic media.

Video that has been saved for internal personnel investigations will be used internally by ICE. Video of possible criminal or terrorist activities may be used internally or may be transferred to an external investigating entity for investigation. Once transferred to an external investigating entity, the video is no longer under the control of ICE and may be used and shared by that entity consistent with their investigative policies and procedures. Before video may be disclosed to an outside entity for investigative purposes, the Assistant Director/OPR, Division Director/OPR/Security, or Deputy Division Director/OPR/SMU must authorize such disclosure. Finally, stored video is not altered or enhanced.

Are there access control policies limiting who can see and use the video images and for what purposes?

Yes. Access to view and use video images is limited to OPR/SMU and PSO personnel with a need to know. Authorized users of the SM-CCTV System will be able to see and use the video in one of two ways: (1) by logging onto an SMS workstation or (2) by viewing displays that feed live video from nearby CCTV cameras. Users are required to enter a unique username and password to access the SMS workstations and the SM-CCTV System. In addition, access to the security command center, which has SMS workstations, is limited to authorized personnel who use their security badge on the electronic badge reader outside the door to access the command center. User roles within the SM-CCTV System also contain controls that limit access and use of the video. Users who are Operators of the SM-CCTV System may view video only from the ICE facility at which they are located. While both Operators and System Administrators can view live and recorded images, the SM-CCTV System prevents Operators from savings copies of video. Additionally, cameras monitor access to the security command center and equipment room containing the DVRs. Finally, OPR/SMU personnel and PSOs may also view live video displays at certain guard posts or offices at ICE facilities. These guard posts and offices are manned by OPR/SMU and PSO personnel or are locked to prevent access when not in use.

Are there auditing mechanisms to monitor who accesses the records, and to track their uses, and if so, are these mechanisms a permanent and unalterable part of the entire system?

Operators of the SM-CCTV System use unique logons at SMS workstations which permit an electronic audit trail traceable to a particular user. Assurances of appropriate use of the system come from peer review of others behavior and periodic review of sample data from the audit logs conducted by the System Administrator. The potential for inappropriate use of the SM-CCTV System's pan/tilt/zoom cameras is limited inside of a security command center users pan, tilt, or zoom the cameras in view of their co-workers. Users outside of a security command center at guard stations may only watch fixed live video feeds. In any security command center, multiple guards are on duty at any one time and they review each other's use of video by virtue of their close proximity to each other and the fact that all video feeds being observed by each individual guard may also be easily seen by the other guards. Additionally there is a camera located in the security command center to monitor the room and what is being viewed on the monitors. This camera records directly to a DVR in the SMS equipment room so that any inappropriate activity is captured. Users are monitored periodically in real time and in the event of suspicious behavior or an allegation of misconduct, a review of recorded video would occur. Finally, there is an additional camera in the equipment room to monitor any physical access to the DVRs.

System Administrators also have unique logon IDs and an audit trail of their logon to SMS created and stored. System Administrator audit logs are reviewed each week by the SMS Information Systems Security Officer.

What training was conducted for officials monitoring or accessing the technology?

Users receive informal hands-on training from the System Administrator who provides instruction for the operation of the system. Users must read and sign a SMS Rules of Behavior document prior to accessing the system.

1.5 What specific legal authorities, arrangements, and/or agreements defined the surveillance system?

- ☐ Legislative authorization at the city or state level
- ☒ Executive or law enforcement decision
- ☐ Decision-making process included public comment or review
- ☒ Entity making the decision relied on:
  - ☒ case studies
  - ☒ research
  - ☐ hearings
  - ☐ recommendations from surveillance vendors
  - ☐ information from other localities
  - ☐ other (please specify)

Funding:
☐ DHS Grant
☐ General revenues
☒ Law enforcement budget
☐ Other (please specify)
☐ Funding has limited duration (please specify)
☐ Funding renewal is contingent on program evaluation

Appendix is attached, including:
- ☐ Authorizing legislation
- ☐ Grant documents
- ☐ Transcript of public hearing or legislative session
- ☐ Press release
- ☐ Program manuals outlining the system's rules and regulations
- ☐ Other (please specify)

1.5.1 The section should also include a list of the limitations or regulations controlling the use of the video surveillance system. This may include existing law enforcement standards, such as subpoenas and warrants, or surveillance-specific rules. For example, is a warrant required for tracking or identifying an individual?

In conducting the activities described in this PIA, both ICE and FPS exercise authority under 40 USC 1315, delegated to them by the Secretary of Homeland Security, to protect the buildings, grounds, and property that are owned, occupied, or secured by the Federal Government and the persons on the property. FPS is delegated this authority pursuant to DHS Delegation Number 17007, "Delegation for the Administration of the Federal Protective Service," which permits FPS to detail its personnel to other agencies for the protection of the property and persons on the property. ICE is delegated this authority pursuant to DHS Delegation Number 0160.1, "Delegation to DHS Organizational Elements," which authorizes the highest ranking official within each Organizational Element to (a) direct, coordinate and administer physical security programs in accordance with applicable DHS management directives; and (b) designate physical security, information security and industrial security officer(s) and submit designations in writing to the DHS Director of Security, with updates as necessary. In addition, 41 CFR 102-81.15 states that a June 28, 1995 Presidential Policy Memorandum for Executive Departments and Agencies titled "Upgrading Security at Federal Facilities" directs executive agencies to upgrade and maintain security in facilities they own or lease under their own authority to the minimum standards specified in Department of Justice's June 28, 1995 study titled "Vulnerability Assessment of Federal Facilities." Also, ICE under DHS has been authorized to collect information under 8 U.S.C. §§ 1103,1105, 1221, 1225, 1281, 1302, 1303, 1304, 1305, 1306, 1324(b)(3), 1324a, 1324c, 1357, 1360(b); 18 U.S.C. Chapter 27; 19 U.S.C. §§ 1431, 1436, 1481, 1484, 1485, 1509; 1584, 1589a, 1592, 1593a; 21 U.S.C. § 967; 31 U.S.C. §§ 5316, 5318; 40 U.S.C. § 1315; and 50 U.S.C. App. § 2411.

The cameras are used within and on exterior perimeters of federal facilities, which have posted signs indicating that individuals are subject to video surveillance. All users must sign SMS Rules of Behavior which details appropriate use of the system.

1.6 Privacy Impact Analysis

Given the amount and type of data collected, and the system's structure, purpose and use discuss what privacy risks were identified and how they were mitigated. If during the system design or technology selection process, decisions were made to limit the scope of surveillance or increase accountability, include a discussion of this decision.
Relevant privacy risks include:

- ***Privacy rights**. For example, the public cameras can capture individuals entering places or engaging in activities where they do not expect to be identified or tracked. Such situations may include entering a doctor's office, Alcoholics Anonymous, or social, political or religious meeting.*

The SM-CCTV System uses cameras to monitor the interior and perimeter of ICE facilities. The purpose of the system is to detect and deter criminal and terrorist activity and to provide investigatory leads only. Cameras are not placed in locations where there is a reasonable expectation of individual privacy, such as bathrooms and changing rooms. Cameras are placed to observe egress/ingress routes into the facility. Cameras are placed to observe traffic in hallways and rooms that are considered sensitive to the operations of ICE. Exterior cameras are located to observe immediate public areas surrounding ICE facilities. This is done to observe any attempt to enter or harm the building and its occupants from outside the building.

- ***Freedom of speech and association**. Cameras may give the government records of what individuals say, do, and read in the public arena, for example documenting the individuals at a particular rally or the associations between individuals. This may chill constitutionally-protected expression and association.*

The system should not restrict freedom of speech or association as the images are only used to detect and deter criminal or terrorist activity and as evidence in criminal, terrorist, or internal disciplinary proceedings. 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 an ICE facility, is not treated differently by ICE than any other activities that may be captured by an SM–CCTV System camera. Unless there is evidence of illegal or suspicious activity and the Assistant Director/OPR, Division Director/OPR/Security, or Deputy Division Director/OPR/SMU gives approval for transferring DVR recordings to a DVD or portable electronic media, video will not be maintained of those images for longer than the storage capacity of the DVR, which is approximately 90-180 days. Video that has been saved for internal personnel investigations will be used internally by ICE. Video of possible criminal or terrorist activities may be used internally or may be transferred to an external investigating entity

for investigation. If transferred to an external investigating entity, the video is no longer under the control of OPR/SMU but will be used and shared in accordance with the entity's investigative policies and procedures. OPR/SMU does not share images or video without a legitimate law enforcement purpose. Requests by external investigative entities for images or video must be made to the Assistant Director/OPR, Division Director/OPR/Security, or Deputy Division Director/OPR/SMU.

- ***Government accountability and procedural safeguards***. *While the expectation is that law enforcement and other authorized personnel will use the technology legitimately, the program design should anticipate and safeguard against unauthorized uses, creating a system of accountability for all uses.*

Operators and System Administrators of the SM-CCTV System have unique logons and an audit trail of their logon is created and stored. Further, the SM-CCTV System prevents Operators from saving copies of video or deleting video. Only System Administrators of the SM-CCTV System, comprised solely of OPR/SMU personnel with the need to know, have the capability to copy video from the DVRs to portable electronic media.

Assurances of appropriate use of the system come from periodic review of sample data from the audit logs conducted by the System Administrator with the possibility of systematic review. Additionally, appropriate use is enforced by peer review of others' behavior. The potential for inappropriate use of the SM-CCTV System is limited as users inside of a security command center pan, tilt, or zoom cameras in view of their coworkers. In any security command center, multiple guards are on duty at any one time and they review each other's use of video by virtue of their close proximity to each other and the fact that all video feeds being observed by each individual guard may also be easily seen by the other guards. Access to the security command center is electronically controlled; authorized personnel use their ICE security badges to enter the room.

Users outside of a security command center at guard stations may only watch fixed live video feeds. All users must read and sign the SMS Rules of Behavior document prior to accessing the system, which informs users about appropriate uses for the system. The misuse of any SMS component will subject personnel to administrative and potentially criminal penalties.

- ***Equal protection and discrimination***. *Government surveillance, because it makes some policing activities invisible to the public, poses heightened risks of misuse, for example, profiling by race, citizenship status, gender, age, socioeconomic level, sexual orientation or otherwise. Decisions about camera placement, and dynamic decisions about camera operation, should be the product of rationale, non-discriminatory processes and inputs. System decisions should be scrutinized with fairness and non-discrimination concerns in mind.*

SM-CCTV System cameras are mounted in elevated areas on the outside of ICE facilities and are placed within ICE facilities to monitor specific entry and exit points to areas of interest

within the facility. SM-CCTV System cameras are not placed in locations where there is a reasonable expectation of individual privacy, such as bathrooms and changing rooms. Cameras are placed to observe entrance into the facility. Cameras are placed to observe traffic in hallways and rooms that are considered sensitive to the operations of ICE. For example, cameras are placed to observe the SMS equipment room that houses the DVRs and the loading dock at PCN where deliveries may be made to ICE headquarters. Exterior cameras are located to observe the immediate area surrounding the ICE facility. This is done to observe any attempt to enter or harm the building and its occupants from outside the building. Cameras are used exclusively for the detection and deterrence of criminal or terrorist activity by PSOs and OPR/SMU personnel, whose subject matter training teaches them to avoid profiling of protected classes of individuals. Camera placement in these areas does not pose a heightened risk of misuse.

Section 2.0 – Uses of the System and Information

2.1 Describe uses of the information derived from the video cameras.

Please describe the routine use of the footage. If possible, describe a situation (hypothetical or fact-based, with sensitive information excluded) in which the surveillance cameras or technology was accessed for a specific purpose.

Information on the video will be used by PSOs and OPR/SMU personnel to detect and respond to potential unauthorized entry and/or unlawful activities in real time within ICE facilities and in the areas surrounding the ICE facilities. As an example, PSOs and OPR/SMU personnel view an individual entering a restricted area after normal business hours wearing a ski mask. Entering a restricted area is not necessarily a cause for alarm, however by using the video the PSOs and OPR/SMU personnel see that the individual is masked and, therefore, there is cause for alarm. Information may also be used to support internal personnel investigations and internal and external law enforcement investigations and prosecutions to the extent it contains information relevant to actual or potential misconduct, criminal, or terrorist activity.

2.2 Privacy Impact Analysis

Describe any types of controls that are in place to ensure that information is handled in accordance with the above described uses. For example, is appropriate use of video covered in training for all users of the system? Are audit logs regularly reviewed? What disciplinary programs are in place if an individual is found to be inappropriately using the video technology or records?

PSOs and OPR/SMU personnel must read and sign a SMS Rules of Behavior prior to using the SM-CCTV System for the first time. The capacity of the DVRs to only hold approximately 90-180 days of video limits the potential for misuse of the information on the video because it is not retained for a significant period of time. Additionally, Operator's audit

logs are reviewed each week by System Administrators and System Administrator audit logs are reviewed each week by the SMS Information Systems Security Officer. PSOs and OPR/SMU personnel are subject to criminal and administrative penalties if they use the system for unauthorized purposes.

Section 3.0 – Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What is the retention period for the data in the system (i.e., how long is footage stored)?

- ☐ 24-72 hours
- ☐ 72 hours – 1 week
- ☐ 1 week – 1 month
- ☐ 1 month – 3 months
- ☒ 3 months – 6 months
- ☐ 6 months – 1 year
- ☐ more than 1 year (please describe)
- ☐ indefinitely

3.1.1 Describe any exemptions for the retention period (i.e. Part of an investigation or review)

The retention period may be exempted during an internal or external investigation. Video that has been saved to portable electronic media for purposes of an internal personnel investigation or an investigation into suspected criminal or terrorist activities may be used internally for investigation or turned over to an outside investigating entity. If turned over to an outside entity, the video is no longer under the control of OPR/SMU but will be used and shared in accordance with the entity's investigative policies and procedures. The Assistant Director/OPR, Division Director/OPR/Security, or Deputy Division Director/OPR/SMU must provide prior approval for video to be saved from the DVR to portable electronic media or for such saved video to be disclosed to external investigating entities.

3.2 Retention Procedure

- ☒ Footage automatically deleted after the retention period expires
- ☐ System operator required to initiate deletion
- ☒ Under certain circumstances, officials may override retention period:
  - ☒ To delete the footage before the retention period
  - ☒ To retain the footage after the retention period
  - ☒ Please describe the circumstances and official process for override

Video is stored for approximately 90-180 days on the DVRs, depending on a variety of factors pertaining to the specific configuration of the cameras the DVR is serving.[3] After that period the oldest video information is overwritten by new incoming video information, unless it has been previously saved to portable electronic media for Suspicious Activity Reporting or investigative purposes. Video recordings are only preserved beyond this period for investigative and evidentiary purposes when they are relevant for internal personnel investigations and actual or suspected criminal or terrorist activity. System Administrators delete video before the retention period only in rare circumstances such as a technical malfunction.

3.3 Privacy Impact Analysis:

Considering the purpose for retaining the information, explain why the information is maintained for the indicated period.

Video is retained only until the DVR is full, at which point the SM-CCTV System automatically begins to overwrite the information. The retention period is approximately 90-180 days. This is an appropriate amount of time in that ICE can still identify potentially relevant video when actual or suspected criminal or terrorist activity has occurred but is not immediately reported or identified.

When a portion of video is being retained for the purposes of satisfying a request for video for either for internal investigations, or other federal, state or local law enforcement investigations, OPR/SMU will save a copy of the relevant portions of the video to a DVD. The Assistant Director/OPR, Division Director/OPR/Security, or Deputy Division Director/OPR/SMU must provide prior approval for video to be saved from the DVR to portable electronic media and for disclosure to external investigating entities.

Section 4.0 – Internal Sharing and Disclosure

The following questions are intended to describe the scope of sharing within the surveillance operation, such as various units or divisions within the police department in charge of the surveillance system. External sharing will be addressed in the next section.

4.1 With what internal entities and classes of personnel will the information be shared?

Internal Entities
- ☒ Investigations unit
- ☐ Auditing unit
- ☐ Financial unit
- ☒ Property-crimes unit
- ☐ Street patrols
- ☒ Command unit

[3] See footnote 1.

☐ Other (please specify)
☐ None

Classes of Personnel
☒ Command staff (please specify which positions)
☒ Middle management (please specify)
☐ Entry-level employees
☒ Other (please specify)

Information collected by the SM-CCTV System is maintained by OPR/SMU. Information from the SM-CCTV system may be provided to investigators of potential criminal, terrorist, or internal personnel incidents within or on the perimeter of ICE facilities. Internal investigators may be from an ICE program office such as OPR or the Office of Homeland Security Investigations. Investigators may also work for the DHS Office of the Inspector General.

4.2 For the internal entities listed above, what is the extent of the access they receive (i.e. what records or technology is available to them, and for what purpose)?

Only copies of the relevant video will be provided for disciplinary, investigatory and/or prosecutorial purposes.

4.2.1 Is there a written policy governing how access is granted?

☒ Yes (please detail)
☐ No

System Administrators will only save video from the SM-CCTV System to portable electronic media when they have been directed by the Assistant Director/OPR, Division Director/OPR/Security, or Deputy Division Director/OPR/SMU. This is specified in the System Security Plan and the system's procedures manual.

4.2.2 Is the grant of access specifically authorized by:

☐ Statute (please specify which statute)
☐ Regulation (please specify which regulation)
☒ Other (please describe)
☐ None

Only the Assistant Director/OPR, Division Director/OPR/Security, or Deputy Division Director/OPR/SMU may direct System Administrators to save a copy of SM-CCTV System video to portable electronic media and disclose it outside of ICE.

4.3 How is the information shared?

4.3.1 Can personnel with access obtain the information:

- ☐ Off-site, from a remote server
- ☒ Via copies of the video distributed to those who need it
- ☐ Only by viewing the video on-site
- ☐ Other (please specify)

4.4 Privacy Impact Analysis:

Considering the extent of internal information sharing, discuss what privacy risks were identified and how they were mitigated. For example, discuss any access controls, encryption, training, regulations, or disciplinary procedures that will ensure only legitimate uses of the system within the department.

Access to the system is restricted to those OPR/SMU and PSO personnel who have a need for access to accomplish their duties, which pertain to physical security of ICE facilities. These users are required to enter a unique username and password to access the SMS workstations and the SM-CCTV System. Individual users receive informal hands-on training from the System Administrator who provides instruction for the operation of the system. Users must also read and sign the SMS Rules of Behavior governing the system. PSOs and OPR/SMU personnel are subject to criminal and administrative penalties if they use the system for unauthorized purposes. Within the system all users can access video stored on the DVRs, however, only System Administrators can save video to portable electronic media. Additionally, written internal procedures require Assistant Director/OPR, Division Director/OPR/Security, or Deputy Division Director/OPR/SMU approval before System Administrators are authorized to transfer video to portable electronic media and disclose it within DHS for the purposes described above.

Section 5.0 – External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to your operation – including federal, state and local government, as well as private entities and individuals.

5.1 With which external entities is the information shared?

List the name(s) of the external entities with whom the footage or information about the footage is or will be shared. The term "external entities" refers to individuals or groups outside your organization.

☒ Local government agencies (please specify): On an ad hoc basis, local law enforcement agencies may be provided access to extracts (copies of limited set of video) from the system to the extent it is relevant to a criminal or terrorism investigation in which those agencies are participating, directing, or supporting. These extracts may be disclosed to a local government agency when the record alone or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

☒ State government agencies (please specify): On an ad hoc basis, state law enforcement agencies may be provided access to extracts (copies of limited set of video) from the system to the extent it is relevant to a criminal or terrorism investigation in which those agencies are participating, directing, or supporting. These extracts may be disclosed to a State government agency when the record alone or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

☒ Federal government agencies (please specify): On an ad hoc basis, federal law enforcement agencies may be provided access to extracts (copies of limited set of video) from the system to the extent it is relevant to a criminal or terrorism investigation in which those agencies are participating, directing, or supporting. Further, extracts of video from the system may be shared with DOJ for prosecutions and with other federal law enforcement organizations for the investigation, prosecution or prevention of criminal acts.

☐ Private entities:
- ☐ Businesses in monitored areas
- ☐ Insurance companies
- ☐ News outlets
- ☐ Other (please specify)

☒ Individuals:
- ☒ Crime victims
- ☒ Criminal defendants
- ☐ Civil litigants
- ☒ General public via Public Records Act or Freedom of Information Act requests
- ☐ Other (please specify)

5.2 What information is shared and for what purpose?

5.2.1 For each entity or individual listed above, please describe:

☐ The purpose for disclosure
☐ The rules and regulations governing disclosure
☐ Conditions under which information will not be disclosed
☐ Citations to any specific authority authorizing sharing the surveillance footage

Disclosure to federal, state and local law enforcement agencies occurs for terrorism and criminal law enforcement purposes only. The requesting agency must receive approval from the Assistant Director/OPR, Division Director/OPR/Security, or Deputy Division Director/OPR/SMU prior to any information being shared with outside agencies. In the course of terrorism or criminal law enforcement and prosecutorial efforts, those agencies may further share video data with crime victims and criminal defendants as is appropriate or required by the relevant criminal rules and procedures. Finally, ICE will release to the public any video that is mandated to be released under the Freedom of Information Act (5 U.S.C. § 552).

5.3 How is the information transmitted or disclosed to external entities?

☒ Discrete portions of video footage shared on a case-by-case basis
☐ Certain external entities have direct access to surveillance footage
☐ Real-time feeds of footage between agencies or departments
☐ Footage transmitted wirelessly or downloaded from a server
☒ Footage transmitted via hard copy
☐ Footage may only be accessed on-site

For purposes of sharing selected portions of video information with entities outside ICE, the selected video portion is saved to portable electronic media, such as a DVD.

5.4 Is a Memorandum of Understanding (MOU), contract, or agreement in place with any external organization(s) with whom information is shared, and does the MOU reflect the scope of the information currently shared?

☐ Yes
☒ No

An MOU is not required to share information with law enforcement organizations on a case-by-case basis where the external law enforcement organization has jurisdiction to collect evidence relevant to terrorist or criminal activity.

5.5 How is the shared information secured by the recipient?

For each interface with a system outside your operation:

☐ There is a written policy defining how security is to be maintained during the information sharing
☐ One person is in charge of ensuring the system remains secure during the information sharing (please specify)
☒ The external entity has the right to further disclose the information to other entities
☐ The external entity does not have the right to further disclose the information to other entities
☐ Technological protections such as blocking, face-blurring or access tracking remain intact one information is shared
☒ Technological protections do not remain intact once information is shared

5.6 Privacy Impact Analysis:

Given the external sharing, what privacy risks were identified? Describe how they were mitigated. For example, if a sharing agreement is in place, what safeguards (including training, access control or assurance of technological privacy protection) have been implemented to ensure information is used appropriately by agents outside your department/agency?

The privacy risk is unauthorized, intrusive or inappropriate usage of the system for personal and/or professional gain, to include the loss or inappropriate use of video records stored on the DVR or retained on portable electronic media such as a DVD for investigative purposes. These risks are mitigated by the Assistant Director/OPR, Division Director/OPR/Security, or Deputy Division Director/OPR/SMU reviewing all requests for video from the SM-CCTV System and approving any disclosures to third-parties of video to ensure it is appropriate and for the purpose of the suspected criminal or terrorist investigation.

Section 6.0 – Technical Access and Security

6.1 Who will be able to delete, alter or enhance records either before or after storage?

☐ Command staff
☐ Shift commanders
☐ Patrol officers
☐ Persons outside the organization who will have routine or ongoing access to the system (please specify)
☒ Other (please specify)

Only System Administrators who are OPR/SMU supervisors are authorized to delete video, and deletion may only occur at the DVR itself. However, video will only be deleted by System Administrators in rare circumstances such as a technical malfunction. Standard procedure is for video to be retained for the 180 day period until it is automatically overwritten. Video stored to the DVRs is not altered or enhanced.

6.1.1 Are different levels of access granted according to the position of the person who receives access? If so, please describe.

☒ All authorized users have access to real-time footage
☐ Only certain authorized users have access to real-time footage (please specify which users)
☒ All authorized users have access to stored data
☐ Only certain users have access to stored data (please specify which users)
☒ All authorized users can control the camera functions (pan, tilt, zoom)
☐ Only certain authorized users can control the camera functions
☐ All authorized users can delete or modify footage
☒ Only certain authorized users can delete or modify footage (please specify which users)

There are two categories of user access that have been incorporated into the SM–CCTV System. The first user category is the System Administrator. System Administrators have full access rights to all of the SM-CCTV System and the capability to save video from DVRs with the approval of the Assistant Director/OPR, Division Director/OPR/Security, or Deputy Division Director/OPR/SMU. In addition, only System Administrators who are OPR/SMU supervisors are authorized to delete video, deletion occurs at the DVR itself, and video will only be deleted in rare circumstances such as a technical malfunction. Standard procedure is for video to be retained for the 180 day period until it is automatically overwritten. System Administrators are responsible for the daily maintenance of the SM-CCTV System and are tasked with all responsibilities associated with user access control.

The second user category is Operator. Operators can access live and recorded video. However, the SM-CCTV System prevents Operators from saving copies of video. In addition, OPR/SMU policy prohibits users from deleting video and video can only be deleted at the DVR itself. Physical access to the DVRs is monitored by camera.

6.1.2 Are there written procedures for granting access to users for the first time?

☐ Yes (please specify)
☒ No

To gain access to SM-CCTV System, users must be PSOs or OPR/SMU personnel with a valid need-to-know and related job responsibility, which is verified through their supervisors. Once an access request has been processed and granted, the individual will receive informal hands-on training from the System Administrator who provides instruction for the operation of the system and must read and sign the SMS Rules of Behavior governing the system. SM-CCTV System Administrators only grant access privileges to an individual who holds an active account for the ICE Network, which means the individual has already successfully undergone a background check by ICE. Once an individual's credentials have been verified, all operations associated with granting access are manually performed by a System Administrator.

6.1.3 When access is granted:

☐ There are ways to limit access to the relevant records or technology (please specify)
☒ There are no ways to limit access

6.1.4 Are there auditing mechanisms:

☒ To monitor who accesses the records?
☐ To track their uses?

Operators of the SM-CCTV System use a unique log in at SMS workstations which permits an electronic audit trail identifiable to a particular user. Assurances of appropriate use of the system come from peer review of others behavior and periodic reviews of sample data from the audit log by the System Administrator. The potential for inappropriate use of the SM-CCTV System's pan/tilt/zoom cameras is limited as users inside of a security command center pan, tilt, or zoom the cameras in view of their co-workers. Users outside of a security command center at guard stations may only watch fixed live video feeds. In any security command center, multiple guards are on duty at any one time and they review each other's use of video by virtue of their close proximity to each other and the fact that all video feeds being observed by each individual guard may also be easily seen by the other guards. Additionally there is a camera located in the security command center to monitor the room and what is being viewed on the monitors. This camera records directly to a DVR in the SMS equipment room so that any inappropriate activity is captured. Users are monitored periodically in real time and in the event of suspicious behavior or an allegation of misconduct, a review of recorded video would be made. Finally, there is an additional camera in the equipment room to monitor any physical access to the DVRs.

While both System Administrators and Operators may access recorded video from the DVRs, only System Administrators have the ability to retrieve and save stored video to portable electronic media. As with Operators, System Administrators have unique logons and an audit trail of their logons is created and stored. This includes any access, duplication, or deletion of recorded video.

Operator audit logs are reviewed each week by System Administrators and System Administrator audit logs are reviewed each week by the SMS ISSO. The SMS audit logs are maintained in accordance with the existing ICE system maintenance policies and procedures. The SMS Security Plan specifies that backup copies of audit records are retained for five years. Also, any system security violation or suspected misuse is reported to the Office of the Information System Security Manager in accordance with the DHS security standards, as well as to OPR/SMU.

6.1.5 Training received by prospective users includes discussion of:

☐ Liability issues
☒ Privacy issues
☒ Technical aspects of the system
☒ Limits on system uses
☒ Disciplinary procedures
☐ Other (specify)
☐ No training

The training lasts:

☐ None
☐ 0-1 hours
☐ 1-5 hours
☒ 5-10 hours
☐ 10-40 hours
☐ 40-80 hours
☐ More than 80 hours

The training consists of:

☐ A course
☐ A video
☒ Written materials
☐ Written materials, but no verbal instruction
☐ None
☒ Other (please specify)

All ICE personnel and contractors complete annual mandatory privacy and security training. All personnel who access SMS are required to sign a SMS Rules of Behavior document, which includes provisions regarding appropriate use of the system and obligations to protect sensitive information from disclosure to unauthorized individuals or groups. After the SMS Rules of Behavior have been signed, authorized users are presented with informal system-specific training by the System Administrator.

6.2 The system is audited:

☒ When an employee with access leaves the organization
☐ If an employee is disciplined for improper use of the system
☒ Once a week
☐ Once a month
☐ Once a year
☐ Never
☒ When called for

6.2.1 System auditing is:

☒ Performed by someone within the organization
☐ Performed by someone outside the organization
☐ Overseen by an outside body (for example a city council or other elected body – please specify)

6.3 Privacy Impact Analysis:

Given the sensitivity and scope of information collected, what privacy risks related to security were identified and mitigated?

The primary privacy risk associated with this system is that personally identifiable information will be used inappropriately. This is mitigated by system access controls, user training, peer supervision and audit trail monitoring. The network connections for the entire SM-CCTV System are operated and maintained by the appropriate individuals within OPR/SMU. Specifically, SMS is connected to the ICE network via encrypting firewalls which use federally required FIPS 140-2 certified encryption modules and Advanced Encryption Standard 128-bit encryption keys to create an encrypted tunnel within the ICE network solely to connect SM-CCTV System between ICE facilities. The risk of unauthorized access to the SM-CCTV System video feed is also mitigated by the fact that cable used for video feeds is enclosed in special tubing designed to detect tampering.

While both Operators and System Administrators may access recorded video from the DVRs, only System Administrators can save video to portable electronic media. Both Operators and System Administrators have unique logons and an audit trail of their logon is created and stored. The potential for inappropriate use of the SM-CCTV System is limited as users inside of a security command center pan, tilt, or zoom cameras in view of their coworkers. Users outside of a security command center at guard stations may only watch fixed live video feeds. In any security command center, multiple guards are on duty at any one time and they review each other's use of video by virtue of their close proximity to each other and the fact that all video feeds being observed by each individual guard may also be easily seen by the other guards.

Further, all users have had their credentials verified, and are current on Information Assurance training requirements. Audit logs of system logon by Operators and System Administrators and access to a security command center by all users are maintained and reviewed to further limit the risk of PII misuse. The nature of this video recording prohibits the ability to retrieve video information by the name of an individual or some identifying number, symbol or other particular assigned to the individual.

Section 7.0 – Notice

7.1 Is notice provided to potential subjects of video recording that they are within view of a surveillance camera?

☒ Signs posted in public areas recorded by video cameras
☐ Signs in multiple languages
☒ Below is a copy of the wording of such notice signs
☐ Notice is not provided
☐ Other (please describe)

U.S. Government Property. This facility may be protected by video surveillance. To report an emergency or incident, contact Federal Protective Service (877) 437-7411. WARNING: Criminal offenses committed on these premises will be prosecuted under Federal Law.

Section 8.0 – Technology

The following questions are directed at analyzing the selection process for any technologies used by the video surveillance system, including cameras, lenses, and recording and storage equipment.

8.1 Were competing technologies evaluated to compare their ability to achieve system goals, including privacy protection?

☐ Yes
☒ No

8.2 What design choices were made to enhance privacy?

☐ The system includes face-blurring technology
☐ The system includes blocking technology
☐ The system has other privacy-enhancing technology (Please specify)
☒ None (Please specify)

Responsible Officials

Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature Page

_____

Mary Ellen Callahan

Chief Privacy Officer

Department of Homeland Security