Federal Trade Commission

Privacy Impact Assessment

FTC Access Control System

April 2014

1 Overview

This document is a Privacy Impact Assessment (PIA) for the FTC's Access Control System (ACS). The ACS is a suite of hardware (e.g., scanners, video cameras, dedicated servers and peripheral computers, keys and locking mechanisms, support kiosks) and software used by the FTC Security Office to secure, monitor, and control access to all FTC facilities and designated areas within those facilities. ACS functions include monitoring the perimeter of FTC buildings and facilities and controlling physical access to such buildings and facilities by FTC employees, contractors, and visitors. The ACS is currently operating at the FTC's Washington, DC, facilities, including FTC Headquarters, leased space at Constitution Center (CCenter), and the FTC warehouse. ACS will eventually be deployed to all FTC Regional Offices and designated areas within those facilities.[1]

The ACS has three main components: (1) the Physical Access Control System (PACS), which generally controls and keeps electronic logs of when individuals enter and exit FTC facilities; (2) the Closed Circuit TV (CCTV) system, which maintains video recordings of designated areas within and outside FTC facilities; and (3) the Electronic Key Management (EKM) system, which maintains records of employees or contractors who have been issued FTC office keys and when such individuals use their keys to access such offices.

In addition, when the FTC is a tenant or occupant in commercially leased or other non-FTC-owned properties, the property owner or property management may independently maintain and operate its own access control system for individuals entering and exiting those properties. For example, the CCenter (see above) maintains and operates its own Physical Access Control System (CCenter PACS), which is separate from the FTC's ACS, but is also discussed in this PIA.[3]

This PIA describes the personally identifiable information (PII) that ACS (and the CCenter PACS) collects, maintains, and uses, potential risks to such PII, and how the FTC mitigates those risks to ensure that the privacy of individuals is adequately addressed.[4] As described more fully below, ACS uses electronic data from personal identity verification (PIV cards issued to FTC employees and long-term contractors under HSPD-12[5]) or from authorized proxy cards (issued to other short-term or regular contractors or guests) to verify identity and authority to access FTC facilities and designated internal locations, together with information

[1] As the ACS is implemented in FTC Regional Offices, this PIA will be updated accordingly.

[3] The FTC Security Office, in consultation with the FTC Chief Privacy Officer, have coordinated with CCenter management to determine and establish what information their system collects from FTC employees, contractors, and visitors, what access authorized FTC Security Office personnel will have to their system, and other matters potentially affecting privacy, as described in this PIA.

[4] Although the FTC does not maintain or operate the CCenter PACS, this PIA describes the PII collected, maintained and used by that system, based on information provided by CCenter management, and the steps the FTC has taken within its authority and control to mitigate privacy risks associated with that system. Likewise, while Federal law and policy does not require the FTC to conduct a PIA for employee or contractor data, see section 208 of the E-GOV Act; Office of Management & Budget (OMB), Memorandum 03-22, the FTC, to promote privacy and transparency, has broadened the scope of this PIA to include all individuals whose PII may be collected, maintained or used by the ACS or CCenter PACS.

[5] See Personal Identity Verification (PIV) System Privacy Impact Assessment, http://www.ftc.gov/os/2008/02/hrpd12pia.pdf

regarding any additional keys, pass cards, or similar access-control items that have been issued. For other visitors to FTC facilities, ACS collects identifying information provided directly by the visitor to verify identity and document access. Similar information is collected by the CCenter PACS, as described below, from FTC employees, contractors, and visitors.

2 Information Collected and Stored within the System

2.1 What information (PII) is to be collected, used, disseminated, or maintained by the system?

Physical Access Control System for FTC facilities (PACS)

PACS collects and maintains the following information about FTC employees and contractors who use their PIV cards to enter FTC facilities, to verify the individual's identity and authority to access the facility:

Last Name	First Name
Middle Name	Agency Code
System code	Card Number
Certificate	Personnel Type
Record ID	Activation Date
Expiration Date	Photo
Date/Time Entered and Exited[6]	

In addition, PACS collects, updates, and stores the "Revoked Certificate List," which is used to verify that an individual PIV card is valid (see 2.2 below).

PACS also collects and maintains the following information about individuals who use authorized, or otherwise controlled by FTC, proxy cards:

Last Name	First Name
Card Number	Date/Time Entered/Exited[7]

PACS collects and maintains the following information about visitors to the FTC to verify the identity and document access to the FTC facility:

Last Name	First name
FTC Point of Contact	Purpose of visit
Date	Time entered/exited

For Constitution Center visitors such as couriers or individuals delivering filings to the FTC, the individual submits their government-issued identification card (e.g., driver's license) to the FTC security guard in exchange for an electronic visitor proxy card. When exiting the FTC facility, the individual returns the proxy card to the security guard, in order to receive his or her government-issued identification card.

PACS collects and maintains the following information about FTC employees and visitors authorized to use the FTC Headquarters garage:[8]

[6] Some but not all secure locations collect time-exited as well as time-entered information.
[7] See footnote 6.

Vehicle make	Model
License Plate Number	State
Date	Time entered/exited

In addition, PACS also collects and stores login credentials for FTC staff who are authorized to access or administer PACS, e.g., Chief Security Officer (CSO), Security Specialist, contractor Security Officers, and security maintenance technicians.

Closed Circuit TV (CCTV)

The FTC Security Office places security cameras around the perimeter and inside FTC facilities, including the Childcare Center playground, HQ garage, building exits, Constitution Center, Regional Offices, and other secured areas (e.g., FTC warehouse). The Security Office also has access to security cameras in FTC-leased facilities. The FTC uses the video feeds captured through CCTV for security and law enforcement purposes. Cameras are not placed in places that have reasonable expectations of privacy, such as bathrooms, personnel offices, or changing rooms.

Electronic Key Management (EKM)[9]

The following information is collected and maintained for the key management portion of the ACS:

Name of FTC employee/contractor	Key number
Date/Time individual accesses the room	Room(s) individual can access

Constitution Center Physical Access Control System (CCenter PACS)

The Constitution Center building access control system (CCenter PACS) collects and maintains the following information about FTC employees and contractors who use their PIV or proxy cards to access the shared facility space:

Last Name	First Name
Middle Name	Agency Code
System code	Card Number
Certificate	Expiration Date
Date/Time entered and exited	Photo

CCenter PACS collects and maintains the following information from FTC visitors at its Constitution Center offices:

Last Name	First name
Agency	Purpose of visit
Date	Time entered/exited
Name of person visited	

2.2 What are the sources of the information in the system?

[8] This information is manually logged by the security guard in paper format.
[9] EKM keys are issued only to FTC employees and contractors, and EKM keys are not issued to the public.

PACS

The information in the PACS database for FTC employees and contractors is collected from individual PIV cards, proxy cards, and from the security orientation forms. In addition, PACS collects, updates, and stores the "Revoked Certificate List," which is used to verify that an individual PIV card is valid. This list is downloaded into the PACS from the Federal Bridge Certification Authority (FBCA).

The information in the visitor management portion of the PACS database is collected from the FTC employee sponsoring the visitor and directly from the visitor.

The Security Officers in the Headquarters parking garage obtain information on vehicles parking in the garage from records maintained by Customer Services, from the vehicles entering the garage, and directly from FTC employees and contractors who are permitted to use the garage.

CCTV

CCTV cameras collect video images through real-time monitoring with streaming and storage capabilities; both functions are accessible only by authorized Security Office personnel, and stored images may be reviewed later. CCTV systems record video from a variety of ranges and with differing zooming capabilities, which allows the Security Officer monitoring the CCTV feed to adjust the camera in real-time. The Security Office does not operate or control any CCTV cameras operated by building management in leased buildings but may have access to live feeds and stored images for particular matters affecting FTC security.

EKM

The information in the EKM database is collected from the FTC staff or contractor and from the FTC manager or Administrative Officer who authorizes access to a particular FTC room.

CCenter PACS

The information necessary for FTC employees and contractors to access the Constitution Center building and common areas is provided to Constitution Center Security by the FTC Security Office. Information on visitors to FTC facilities at Constitution Center is collected from the sponsoring FTC employee and the visitor.

2.3 Why is the information being collected, used, disseminated, or maintained?

PACS

The information is used to control access by, and to record the identity of, federal employees, contractors, vendors, and visitors who are authorized to enter FTC facilities, including records of the date/time of such entry. The information is also used to verify that the individual has the correct access privileges and for accountability, if necessary, during building emergencies. The PACS also monitors activity within sensitive areas (access-controlled areas inside FTC facilities) and records names, PIV card or key number, date, and time of entry of the authorized individual entering the area.

CCTV

The closed-circuit security video is recorded and used for FTC security and law enforcement purposes.

EKM

The information is used to assign electronic keys to FTC employees and contractors to ensure that they have appropriate access to internal FTC locations.

CCenter PACS

The information is used to control access by, and to record the identity of, federal employees, contractors, vendors, and visitors who are authorized to enter FTC facilities at Constitution Center, including records of the date/time of such entry. The information is also used to verify that the individual has the correct access privileges and for accountability, if necessary, during building emergencies.

2.4 How is the information collected?

PACS

Personal data on PIV cards are collected from FTC employees and contractors as described in the PIA for FTC's HSPD-12 PIV card program.[10] The PACS captures PIV card data when cardholders swipe their card across the electronic scanners at FTC building entrances and secure areas. The PIV card certificate is checked against the "Revoked Certificate List" to verify that the PIV card is valid. Once the PIV card is confirmed to be valid, its information is used to identify the individual and the authority to access the particular FTC facilities or secure areas where the scanner is located.

The PACS also captures proxy card data when cardholders swipe their proxy cards across the electronic scanners setup at FTC building entrances and secure areas. The proxy card is matched against the assigned database record to identify the individual and the authority to access.

The visitor management portion of PACS collects information that has previously been obtained from the visitor and forwarded to the system by FTC employees for matching against the Federal or state credentials provided by the visitor at the time of the visit. The Security Officer inspects the visitor's credential, matches it to the visitor's data in PACS, and notifies the FTC Point of Contact (POC) of the visitor's arrival.

Vehicles parked in the FTC garage have the vehicle information collected directly from the Administrative Services Office and manually from the driver at the time of entry.

CCTV

CCTV systems collect and record video images from a variety of ranges and with differing zooming, panning, and focusing capabilities.

[10] http://www.ftc.gov/sites/default/files/attachments/privacy-impact-assessments/hrpd12pia.pdf

EKM

The information is collected directly from the FTC staff or contractor and from the manager or Administrative Officer who authorizes access to key-controlled areas.

CCenter PACS

The CCenter PACS captures PIV card data when cardholders swipe their card across the electronic scanners at the Constitution Center building entrances and secure common areas. The card certificate is checked against the "Revoked Certificate List" to verify that the PIV card is valid. Once the PIV card is confirmed to be valid, its information is used to identify the individual and verify the individual's authority to access the Constitution Center building and common areas. The FTC's Security Office delivers the encrypted PACS information to CCenter PACS in person for manual uploading into the CCenter system. As employees and contractors join or leave the FTC, the PACS information is updated, as is the CCenter PACS information.

The CCenter PACS captures proxy card data when cardholders swipes their card across the electronic scanners at the kiosks setup at the Constitution Center building entrances and secure areas. The proxy card is matched against the assigned database record for authorization and access privileges.

The visitor management portion of CCenter PACS collects information that has previously been obtained from the visitor and forwarded by FTC employees for matching against the Federal or state credentials provided by the visitor at the time of the visit. Once the CCenter PACS Security Officer inspects the visitor's credential and matches it against the visitor's data in the system, the Security Officer notifies the FTC point of contact (POC) of the visitor's arrival.

2.5 How will the information be checked for accuracy and timeliness (currency)?

PACS

FTC employees and contractors have the opportunity to verify their data for accuracy when they are issued PIV or proxy cards. Individuals can also review, correct, or update their PACS data at the FTC Security Office at any time.

Visitors to FTC facilities are checked-in using their Federal or state identification against the information provided prior to their visit, but that information is not subsequently updated or revised.

Login credentials, which permit authorized users to access PACS, are not subject to accuracy or timeliness checks, as these credentials are managed directly by each authorized Security Office user. When authorized users leave the FTC or no longer need access to PACS in connection with job functionality, their access rights are revoked.

CCTV

The FTC CCTV cameras collect real-time video of the activities occurring within their viewing space in or near its facilities. The video images are altered through a compression algorithm for storage purposes but otherwise not modified or changed, and only authorized security personnel have access to the stored video data.

EKM

The FTC employee or contractor signs a form accepting responsibility for the key, and the Security Office confirms that the name in the system matches the name on the form. The name and key assignment(s) can later be revised or corrected by the employee's or contractor's Administrative Officer or the Security Office.

CCenter PACS

FTC employees and contractors can check their PIV or proxy cards for accuracy when their badges are issued and can check at any time with the FTC Security Office to revise or update their information.

Visitors and contractors can check their information for accuracy when temporary access credentials are issued.

2.6 Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?

PACS

The FTC has previously used access control systems and video, but the single, comprehensive ACS allows the FTC to integrate its previously separate systems into a single security management solution. This integration should not create any additional privacy concerns.

CCTV

The FTC has previously used video technology but had not integrated CCTV with its PAC system. This integration should not create any additional privacy concerns.

EKM

The FTC has previously used EKM as an isolated Security Office system, but the updated version is web-based and uses secure transmission and encryption. To reduce any privacy risks associated with moving to the web-based system, the FTC only collects the minimum amount information needed for access.

CCenter PACS

The FTC will use access control systems provided by building management at several leased locations. To reduce any additional privacy risks associated with third-party access to and use of FTC data for access control purposes, the FTC and building management will collect and share the minimum information necessary to verify identity, FTC has instructed building management that such data is not to be shared for anything other than security and law enforcement purposes.

2.7 What law or regulation permits the collection of this information?

- 5 U.S.C. § 301, "Government Organization and Employees";
- Executive Order 12977, "Interagency Security Committee";
- Presidential Decision Directive PDD/NSC 12, "Security Awareness and Reporting of Foreign Contacts";
- Homeland Security Presidential Directive 7 (HSPD-7), "Critical Infrastructure Identification Prioritization and Protection";
- National Infrastructure Protection Plan, Government Facilities Sector, Sector-Specific Plans";
- Interagency Security Committee Standard, "Physical Security Criteria for Federal Facilities," April 2010; and
- Federal Property Regulations (General Services Administration), see 41 CFR part 102-74 (facility management).

2.8 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

PACS

The principal privacy risks are the inadvertent or unauthorized access to or disclosure of FTC employee, contractor, or visitor data. To reduce privacy risks, PACS collects and maintains only the minimum amount of personal information that is necessary to verify and grant physical access to FTC facilities and internal FTC locations. In addition, PIV cards are deactivated and returned to the FTC when an FTC employee or contractor leaves the Agency, and access rights are updated when an FTC employee no longer needs physical access to FTC buildings and internal FTC locations. Finally, access to PACS is limited to authorized Security Office users, with the level of access limited to the minimum amount necessary to perform that user's job responsibilities.

The PACS also captures information when proxy cards are issued to temporary users and when those users swipe their cards across the electronic scanners setup at FTC building entrances and secure areas. The proxy card is matched against the assigned database record for authorization and access privileges. To reduce this risk, PACS collects and maintains only the minimum amount of personal information that is necessary to verify identity and issue proxy cards for physical access to FTC facilities or specific internal FTC locations.

Minimal information is collected from visitors coming to the FTC and only the visitor's name and visit date are displayed on the visitor pass. That information is retained only as needed for records and security purposes.

There is also a risk associated with the accuracy of data included in the PACS. Although most of the PII data is provided by the individuals themselves, it is possible that data could be inaccurately entered and mistakenly associated with the wrong individual. To reduce the risk of data being inaccurately entered or incorrectly associated, electronic data collection tools are used to the greatest extent possible, and authorized Security Office users are trained to use the system, periodically receive refresher training, and are reminded of the importance of collecting and maintaining accurate information.

CCTV

The security cameras could collect more information than is necessary to accomplish the security and law enforcement purposes for which they are used. This risk is reduced by placing security cameras in public places only, as opposed to areas such as bathrooms and similar areas where individuals have a reasonable expectation of privacy. Only authorized Security Office personnel have access to live video feeds and stored images, and footage not need for security and law enforcement purposes is routinely destroyed or automatically overwritten.

EKM

The main privacy risk is the use of a valid key for access by an unauthorized user, whether by borrowing another user's key or finding a lost, misplaced, or stolen key, if such use is then mistakenly attributed to the employee or contractor who was assigned the key. This risk is mitigated by having FTC employees or contractors sign Rules of Behavior (RoB), which requires them to maintain possession and control of the key, limit lending or borrowing keys to very narrow circumstances, and require, consistent with FTC incident reporting policy, prompt notification to the Help Desk of a lost key. Upon notification, the EKM manager initiates an immediate protocol to deactivate a misplaced, lost, or stolen key, to prevent unauthorized access.

CCenter PACS

The principal privacy risks are the inadvertent or unauthorized access to or disclosure of FTC employee, contractor, or visitor data. To reduce this risk, the CCenter PACS collects and maintains only the minimum amount of personal information that is necessary to verify and grant physical access to the Constitution Center building and to secured common areas. In addition, PIV cards are deactivated and returned to the FTC when an FTC employee or contractor leaves the Agency, and access rights are updated when an FTC employee or contractor no longer needs physical access to Constitution Center.

The CCenter PACS also captures information when proxy cards are issued to temporary users and when those users swipe their cards across the electronic scanners setup at Constitution Center building entrances and secure areas. The proxy card is matched against the assigned database record for authorization and access privileges. To reduce privacy risks, CCenter PACS collects and maintains only the minimum amount of personal information that is necessary to verify identity and issue proxy cards for physical access to Constitution Center.

Minimal information is collected from visitors coming to visit the FTC at Constitution Center, and only the visitor's name and visit date are displayed on the visitor pass. That information is retained only as needed for records and security purposes.

There is also a risk associated with the accuracy of data included in the CCenter PACS. Although most of the PII data is provided by the individuals themselves, it is possible that data could be mistakenly associated with the wrong individual having identical or similar names could be inaccurately entered. To reduce the risk of data from PACS being inaccurately entered or incorrectly associated and replicated in CCenter PACS, automated electronic data collection tools (e.g., card readers) are used to the greatest extent possible, and authorized users are reminded by the Chief Security Officer to identify, avoid, and correct such errors.

3 Use and Access to Data in the System

3.1 Describe how information in the system will or may be used.

PACS

See Section 2.3 above. Information collected by PACS is used by the FTC Security Office for security and law enforcement purposes.

CCTV

Live and stored video images from CCTV are used for security and law enforcement purposes.

EKM

The information in the system is used for security purposes, to program keys to permit authorized access to designated FTC rooms, and EKM records may be accessed for law enforcement purposes, if necessary.

CCenter PACS

See 2.3 above and the section on PACS in 3.1. Information collected by CCenter PACS is used for security and law enforcement purposes.

3.2 Which internal entities will have access to the information?

PACS

The FTC CSO, FTC Senior Security Specialist, and authorized security maintenance personnel will have administrative access to PACS data. Other authorized Security Office personnel, including the contract security force, will have user access to the system. Authorized OCIO personnel will have access to the system to perform patching. In addition, PACS data may be disclosed (e.g., to the FTC Office of Inspector General (OIG)) for investigative and law enforcement purposes.

CCTV

The FTC CSO, FTC Senior Security Specialist, and authorized security maintenance personnel will have administrative access to the PACS data. The authorized security specialist and authorized contract security officers will have user access. Video clips may be shown to FTC management as needed. CCTV data may be accessed (e.g., by the OIG) for investigative and law enforcement purposes.

EKM

The FTC CSO, FTC Senior Security Specialist, and authorized security maintenance personnel will have administrative access to the data. This data may be accessed (e.g., by the OIG) for investigative and law enforcement purposes.

CCenter PACS

The FTC CSO, FTC Senior Security Specialist, and authorized security maintenance personnel can request administrative access to the data from the Constitution Center access

control technicians or system administrators. This data may be accessed (e.g., by the OIG) for investigative and law enforcement purposes.

3.3 Which external entities will have access to the information?

PACS

Authorized federal, state, and local law enforcement officials may submit an official request to the FTC's Chief Security Officer to access the PACS data. All other external requests must be made through the FTC's FOIA/Privacy Act office. See the FTC's official FOIA page.

CCTV

Authorized federal, state, and local law enforcement officials may submit an official request to the FTC's Chief Security Officer to access the CCTV video images. All other external requests for access must be made through the FTC's FOIA/Privacy Act office. See the FTC's official FOIA page.

EKM

Authorized federal, state, and local law enforcement officials may submit an official request through the FTC's Chief Security Officer to access the EKM data. All other external requests for access must be made through the FTC's FOIA/Privacy Act office. See the FTC's official FOIA page.

CCenter PACS

The CCenter provides access under circumstances to the Constitution Center's Facility Security Committee (FSC), which consists of delegates from each of the tenants in the federally-shared building. The FSC determines the building security procedures and may request the data from building management itself or on behalf of a special tenant, for auditing and/or review purposes. Federal, state, and local law enforcement may submit a request to the FSC for access to the data. All other requests for access must be made through the FTC's FOIA/Privacy Act office, which may need to refer the request to the designated non-FTC entity or entities that operate or have access to CCenter PACS. See the FTC's official FOIA page.

Notice and Access for Individuals

4.1 How will individuals be informed about what information is collected, and how this information is used and disclosed?

PACS

The FTC notifies its employees and contractors at the time it collects the PIV or proxy card data of the purposes for which such data may be used. Additional notice about the collection and maintenance of their data in the System is provided by the applicable Privacy Act system notice (SORN II-11 -- Personnel Security, Identity Management, and Access Control Records System[11]).

[11] http://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems See also Section 8 of this PIA.

CCTV

Not applicable. Statements required under the Privacy Act of 1974, see 5 U.S.C. 552a(e)(3), to inform individuals of the authority, purposes, routine uses, and consequences of collection generally apply when collecting information from individuals on the form used to collect the information, and only for systems of records retrieved by name or other personally assigned identifier. CCTV records are not maintained or retrieved by name or other personally assigned identifier. Furthermore, as noted earlier, cameras are placed only in areas where individuals have no reasonable expectation of privacy (e.g., public perimeter of buildings, and no areas within buildings such as bathrooms, personal offices, changing rooms).

EKM

The FTC employee or contractor signs a form accepting responsibility for the key and agreeing to abide by applicable Rules of Behavior and FTC policies. That form includes a Privacy Act notice explaining authority, purpose, use, etc.

CCenter PACS

As noted above, the FTC provides its employees and contractors with notice when collecting PIV card or proxy card data that may be captured by the CCenter PACS. Additional notice may be provided to such individuals or others (e.g., visitors) by the operator of the CCenter PACS designated by building management. (As the CCenter PACS is not an FTC system of records, no such notice by the FTC is required by the Privacy Act of 1974. (See below, Section 8.)

4.2 Do individuals have the opportunity and/or right to decline to provide information?

PACS

No, FTC employees and contractors who routinely access FTC buildings are legally required to have and use PIV cards or proxy cards to gain such access and may also be required to use PIV cards or proxy cards on card readers to access certain internal FTC locations.

Yes as to visitors, but visitors who decline to provide information will not be permitted access to FTC facilities.

CCTV

No.

EKM

No. FTC employees and contractors who require key-controlled access to FTC facilities must provide certain information to be assigned a key, and the system automatically records when the individual uses the key.

CCenter PACS

No, FTC employees and contractors who routinely access FTC buildings are required to have and use PIV or proxy cards to gain access to the building and may also be required to use PIV cards or proxy cards on card readers to access certain internal FTC locations.

Yes as to visitors, but visitors who decline to provide information will not be permitted access to the Constitution Center building by building management.

4.3 Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?

No. All information provided to or collected by PACS, CCTV, EKM and CCenter PACS may be used for security and law enforcement purposes.

4.4 What are the procedures that allow individuals to gain access to their own information?

PACS

Identification data on PIV and proxy cards are collected at the time the PIV or proxy card is issued, and FTC employees and contractors have access to, and are required to verify, their data as part of the PIV or proxy card issuance process. FTC personnel who later realize that data is incorrect on their badge may contact the FTC Security Office directly.

Visitors are allowed to review the information collected or provided during the sign-in process. Visitors who wish to get a copy of their information at a later date should contact the FTC's FOIA/Privacy Act office, which shall determine whether to grant or deny access as required or authorized by law. See the FTC's official FOIA page.

CCTV

Individuals may request access to CCTV information about themselves, if any, by contacting the FOIA/Privacy Act office. See the FTC's official FOIA page. Requesters should be aware that CCTV systems do not record or retrieve information by personal identifiers. Accordingly, the FTC may be unable to identify a particular video, if any, pertaining to the requesting individual. Additionally, videos are only stored for a maximum of six months and in some cases, a much shorter period, depending on the age and condition of the equipment.

EKM

FTC employees and contractors may contact the FTC Security Office directly.

CCenter PACS

FTC employees and contractors may contact the FTC Security Office directly for information collected by the Constitution Center access control system. Visitors may request access to their information by contacting the FOIA/Privacy Act office, which may need to refer the request to the designated non-FTC entity or entities that operate or have access to CCenter PACS. See the FTC's official FOIA page.

4.5 Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.

The privacy risk of providing individuals with access to their own records is relatively low, as individuals do not have direct electronic access to any of the system components

discussed above, and the risk is limited to the FTC inadvertently providing information to an unauthorized requester in response to a FOIA/PA request. To mitigate such risk, the FTC collects and maintains only the minimum information necessary in the system, limits access privileges to authorized Security Office personnel, and, as noted above, prevents individuals from accessing the system directly. In response to a FOIA/Privacy Act request, the FTC's FOIA/Privacy Act office may also attempt to verify the identity of the requester before disclosing legally accessible records from the system, if any.

5 Web Site Privacy Issues

5.1 Describe any tracking technology used by the Web site and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, Web beacon).

Not applicable—none of the ACS components have any web-based or other means for individuals (employees, contractors, visitors) to directly access the system, as noted in Section 4.5, above. Any tracking technology encountered by authorized FTC personnel when accessing the EKM system would track only their access to and activities within the system.

5.2 If a persistent tracking technology is used, ensure that the proper issues are addressed.

Not applicable.

5.3 If personal information is collected through a Web site, page, or online form accessible through the Internet, is appropriate encryption used? If not, explain.

Not applicable.

5.4 Explain how the public will be notified of the Privacy Policy.

PACS

The Privacy Policy is posted at the main guard post for visitors to see when signing in, and the FTC's Privacy Policy is also available online at www.ftc.gov. In addition, as previously explained, notice is provided to employees and contractors assigned PIV or proxy cards at the time they are issued to these individuals, and in the applicable Privacy Act SORN (see Section 8 below).

CCTV

Not applicable.

EKM

Not applicable. Notice is provided to employees and contractors at the time keys are assigned to individuals (see the Rules of Behavior) and by the applicable Privacy Act SORN, see Section 8 below.

CCenter PACS

The CCenter PACS is not an FTC system. Notice is provided through this PIA, and additional notice may be provided by CCenter building management.

5.5 Considering any Web site or Internet issues, please describe any privacy risks identified and how they have been mitigated.

Not applicable.

5.6 If the Web site will collect personal information from children under 13, or be directed at such children, explain how it will comply with the Children's Online Privacy Protection Act (COPPA).

Not applicable.

6 Security of Information in the System

6.1 Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?

Yes. The FTC follows all applicable Federal Information Security Management Act (FISMA) requirements. The data is categorized as **moderate** using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

6.2 Has a Certification & Accreditation (security control assessment and authorization) been completed for the system or systems supporting the program?

Yes, ACS is a component of the Data Center GSS, the FTC's accredited general support system.

6.3 Has a risk assessment been conducted on the system?

Yes, as part of the Data Center GSS.

6.4 Does the project employ technology that may raise privacy concerns? If so, please discuss its implementation.

Yes. The use of access control systems, visitor management software, and security cameras normally raise privacy concerns. The FTC has addressed these risks and vulnerabilities and subsequent mitigation within this document. For example, all authorized security staff who have access to the system have background investigations and/or have security clearance.

6.5 What procedures are in place to determine which users may access the system and are they documented?

The Chief Security Officer, System Administrator, or authorized Senior Security Specialist issues access roles and privileges based on job requirement. The ACS system user manual documents procedures to limit administrative access to authorized FTC and contractor personnel who need that level of access to perform their job duties.

6.6 Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

All FTC employees and designated contractor personnel are required to complete computer security training and privacy awareness training annually. In addition, Security Office personnel receive specific training on the use of, and issues associated with, each component of the ACS.

6.7 What auditing measures and technical safeguards are in place to prevent the misuse of data?

Auditing measures and technical safeguards are in place commensurate with the National Institute of Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems and Organizations Moderate-Impact Baseline Special Publication (SP) 800-53.

6.8 To whom should questions regarding the security of the system be addressed?

Any questions regarding the security of the system should be directed to the FTC's Chief Information Security Officer.

7 Data Retention

7.1 For what period of time will data collected by this system be maintained?

PACS

Logs for FTC employees, contractors, and visitors are destroyed two years or earlier after final entry or date of document.

CCTV

CCTV video footage is overwritten due to the volume of information in the system. This usually occurs 120 days after the footage was recorded.

EKM

The key holder name and rooms to which the key holder has access are deleted from the EKM system when the key is returned. Written logs of this information are retained for two years. Locks on rooms retain information on the date and time a particular key opened or attempted to open the lock for 2000 transactions (openings/attempted openings) after which the information is overwritten, earliest first.

CCenter PACS

As noted earlier, this system is controlled and operated by CCenter building management. FTC requests removal or deletion of data, as appropriate to minimize unnecessary retention.

Retention of Data for Investigative and Law Enforcement Purposes

Data from PACS, CCTV, EKM, and CCenter PACS may be provided to FTC's OIG and/or entities outside of the FTC for investigative and law enforcement purposes. Information provided to the OIG is retained and disposed of in accordance with FTC records retention schedule N1-122-09-1 approved by the National Archives and Records Administration (NARA).

7.2 What are the plans for destruction or disposal of the information?

Disposal of all information in PACS, CCTV and EKM will be conducted in accordance with FTC policies and procedures and in compliance with Office of Management and Budget (OMB), NARA, and NIST guidelines. FTC instructs Constitution Center building management to dispose of FTC information stored in CCenter PACS in a similar manner.

7.3 Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

See Section 2.8. Destruction of information in PACS, CCTV and EKM occurs within the application automatically or by authorized Security Office and/or OCIO personnel and does not create any additional risk. Written logs are disposed of by shredding on-site by FTC Security personnel or authorized contractors. PIV cards are deactivated and returned to the FTC when an FTC employee or contractor leaves the agency or otherwise no longer needs physical access to FTC buildings.

8 Privacy Act

This section addresses the applicability of the Privacy Act of 1974 to the system, and whether or not the system is covered by a System of Records Notice (mandated for some systems by the Privacy Act of 1974).

8.1 Will the data in the system be retrieved by a personal identifier?

PACS

Yes.

CCTV

No.

EKM

Yes.

CCenter PACS

Yes, but see Section 8.2, below)

8.2 Is the system covered by an existing Privacy Act System of Records notice (SORN)?

Yes, for PACS and EKM. FTC II-11, Personnel Security, Identity Management, and Access Control Records System -- FTC, and VII-3 -- Computer Systems User Identification and Access Records -- FTC (for login credentials of system administrators). These system notices also explain the individual's rights and procedures for reviewing and accessing any records about themselves in the system. FTC II-11 does not apply to CCTV, since these video records are not retrieved from the system by name or other personally assigned identifier subject to the Privacy Act, or to CCenter PACS, which is not an FTC system of records. To the extent that the Office of Inspector General (OIG) retrieves information from PACS, CCTV, EKM or CCenter PACS for investigatory or law enforcement purposes and incorporates such information into OIG records, those records would be covered by FTC I-7 – Office of Inspector General Investigative Files – FTC.

All FTC SORNs are listed and can be downloaded from our public SORN page: http://www.ftc.gov/foia/listofpaysystems.shtm.

9 Privacy Policy

9.1 Confirm that the collection, use, and disclosure of the information in this system has been reviewed to ensure consistency with the FTC's privacy policy.

The collection, use, and disclosure of the identification, authorization, and access data and login credentials described above is consistent with the privacy policy that the FTC provides to the public.

10 Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____
Charles King
Chief Security Officer

Review:

_____ Date: _____
Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____
Peter B. Miller
Chief Privacy Officer

_____ Date: _____
Jeffrey Nakrin
Director, Records and Filings Office

_____ Date: _____
Jeffrey Smith
Chief Information Security Officer

Approved:

_____ Date: _____
Bajinder Paul
Chief Information Officer