Federal Trade Commission
Privacy Impact Assessment

# Electronic Security System fka Access Control System

**Reviewed February 2022**

# 1 System Overview

## 1.1 Describe the project/system and its purpose.

The Access Control System is a combination of hardware (e.g., workstations, servers), software (e.g., security management software), and paper-based information collections (i.e. visitor logs). The Access Control System secures, monitors, and controls access by employees, contractors, visitors, and others to the FTC Headquarters Building (HQ), Constitution Center (CC), warehouse, and designated areas within those facilities.[1]

The Access Control System comprises four major functions: visitor management, physical access control, intrusion detection, and video surveillance. The Access Control System contains personally identifiable information (PII) from FTC employees, contractors, and members of the public who access or attempt to access FTC facilities.

Several individual components comprise the Access Control System, which include (see table):

[1] This PIA addresses the access control measures that are specific to the FTC, but it does not necessarily address access control measures undertaken by entities such as GSA, FPS, or local building security, that apply to all offices in shared buildings (such as CC) in which the FTC has an office. Unless specifically noted in this PIA, security controls in the Regional Offices (RO) are managed by by other entities (such as GSA, FPS, or local building security).

### 1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

- Executive Order 12977, Interagency Security Committee
- Homeland Security Presidential Directive-12, Policies for a Common Identification

**PIV/Proximity Card**

The following data elements are collected from the FTC employee/contractor PIV card and entered into the PACS database at the time of PIV card issuance:

1. Last Name, First Name, Middle Name
2. Agency Code: A four-digit code that is part of the Federal Agency Smart Credential Number (FASC-N) on the card and is assigned by the certificate authority
3. System Code: A two-digit number that is part of the FASC-N
4. Card Number: The number embossed on the PIV card
5. Certificate Number: The certificate number assigned by the certificate authority
6. Personnel Type: Employee or contractor
7. Record ID: A unique number assigned by the PACS and associated with the employee profile
8. Activation Date: Date the profile was entered into the PACS database
9. Expiration Date: Expiration date of the PIV card
10. Employee or Contractor Photograph
11. Date and time the profile was entered into the PACS database

**HQ Visitor Management - Paper Log**

The FTC's visitor management function authorizes and records the entry and exit of visitors requiring temporary access to the HQ building. The security guard verifies the individual's name from any local, State, or Federal government-issued identification (ID) card and enters the information into a hand-written visitor log as a record of the visit. The visitor management function at HQ is governed by the Administrative Manual, Chapter 4: Section 800 – Physical Security. The PII collected from each visitor includes:

1. Date
2. Time of Arrival and Departure
3. Name
4. FTC Point of Contact
5. Name of Firm or Agency

7. Time entered/exited

**Electronic High-Security Key System**

The following information is collected and maintained for the key management system:

1. Name of FTC employee/contractor
2. Date/Time individual accesses the room
3. Key number
4. Room(s) individual can access/room location
5.

### 2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

The system may contain video footage of the interior of FTC buildings. See also section 2.4.

### 2.3 What is the purpose for collection of the information listed above?

The Access Control System is used for employee, intrusion detection, and video surveillance functions at FTC facilities as outlined in this PIA. The Access Control System also serves as a repository for all employee PII required for authorizing and monitoring physical access at FTC facilities.

### 2.4 What are the sources of the information in the system/project? How is the information collected?

| Source of Data | Type of Data Provided & How Its Collected |
|---|---|
| PACS (Server and Database) | x **<u>Employee/Contractor Profiles</u>**. These are manually entered into PACS by Physical Security Branch personnel for each employee/contractor issued a PIV or proximity card. These profiles are used by the card readers to authorize and/or deny access. The information collected is included in Section 2.1 above.<br>x **<u>System Audit Logs</u>**. The PACS server logs all activity to support the requirement to record sufficient information to uniquely identify individuals and the time of access. The system data is never overwritten.<br>x **<u>Physical Security Branch System Administrator and OCIO IT Specialist User IDs</u>**. These are manually entered by OCIO IT Specialists for each employee or contractor who manages employee/contractor profiles, and include individual user names, user IDs, and passwords.<br>x **<u>Contract Security Maintenance Personnel User IDs</u>**. These are manually entered by OCIO IT Specialists and include individual user names, user IDs, and passwords. |
| NVR | x |

| | | |
|---|---|---|
| | | Headquarters parking garage obtain information on vehicles parking in the garage from the vehicles entering the garage and directly from FTC employees and contractors who are permitted to use the garage. |
| Electronic High-Security Key | x | The information in the key management database is |

| | |
|---|---|
| Visitor Logs | x **FTC Physical Security Branch Personnel –** Daily l |

## 4 Notice and Consent

### 4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

Sign-in sheets at FTC HQ visitor entrances are accompanied by a Privacy Act statement to inform individuals entering the building of their rights under the act. (For information about logs in shared buildings, see footnote 1.) When FTC employees or contractors are issued high-security electronic keys, they sign 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 statement. Though not required, as a matter of policy, signs are posted in the FTC HQ lobby to provide notice of surveillance activities via CCTV cameras. In addition, as previously explained, notice is provided to employees and contractors assigned PIV or proxy cards at the time they are issued, and in the applicable Privacy Act System of Records Notice (SORN). (See Section 8.3 of this PIA regarding Privacy Act SORNs.)

☒ Notice is provided via (check all that apply)
- ☒ Privacy Act Statement (☒ Written ☐ Oral)
- ☒ FTC Website Privacy Policy
- ☐

required.  However, as a mat

# 5 Data Accuracy and Security

## 5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

**PACS Server/Database**

FTC employee and contractor profiles are regularly reviewed and audited by Physical Security Branch personnel, and when necessary and approved, updates and/or deletions of information are completed. Information is regularly backed-up as required per the OCIO Contingency Planning Policy.

**Visitor Management (Paper Logs)**

Visitors are required to present some form of official identification to the HQ security guard to ensure that the log contains accurate information about the visitor's identity for security purposes. Changes are not made to the visitor-provided information once entered in the log by the security guard. As noted earlier, visitors can review their log entry to ensure that the HQ security guard has recorded the correct information in the log during their sign-in process.

**NVR (Camera Footage)**

Cameras collect real-time video of the activities occurring within their reviewing space in or near an FTC facility. Cameras may only record what is occurring in real time; there is no editing feature or ability to change the image.

**Electronic High-Security Key**

The FTC employee or contractor signs a form accepting responsibility for the key, and the Facilities or 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.

## 5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

**PACS Server/Database**

Supervisors and/or Contracting Officer's Representatives (CORs) must identify and approve employee/contractor requests to access the PACS server/database and specify the appropriate user role and level of access privileges. Access is based on a valid access authorization and intended system use. All access is based on least-privilege and need-to-know security models. Additionally, auditing measures and technical safeguards are in place commensurate with the Moderate-Impact control Baseline of the National

Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations Special Publication (SP) 800-53.

**Visitor Management (Paper Log)**

Daily, the visitor logs and parking garage records are retrieved from Guard Posts and stored in a locked cabinet for two years, after which time they are shredded by Physical Security Branch personnel.

**NVR**

Only Physical Security Branch (federal personnel) are authorized to access the stored video data, which resides on the NVR hard drives which are physically located in the HQ Data Center. The Data Center is physically accessed via a PIV card and such access is logged on the PACS database. Access to the NVR requires a user ID and password that follows FTC's Access Control Policy. The misuse of any FTC system will subject employees to administrative and potentially criminal penalties. Each user (Physical Security Branch federal employees) has a separate user ID and password for accessing the NVR's data.

**Electronic High-Security Key**

Only Facilities personnel have access to the key software program, which is password protected. The information in the key system is not highly sensitive.

### 5.3 Has the system/project undergone the appropriate security risk assessment and received authority to operate?

Yes. The FTC's Access Control System and its components, all of which are located on FTC premises and managed by FTC personnel, are included in the authorization to operate (ATO) for the Datacenter GSS.

The FTC follows all applicable 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.

### 5.4 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

☒ Not Applicable

## 6 Data Retention and Disposal

### 6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

Information in the Access Control System, including information, if any, that may be incorporated into or otherwise required to be preserved as Federal records, is retained and destroyed in accordance with National Archives and Records (NARA) General Records Schedule (GRS) 5.6, Security Records..

## 7 Website Privacy Evaluation

### 7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

☒ Not Applicable

## 8 Privacy Risks and Evaluation

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

| Risk | Mitigation Strategy |
|---|---|
| **PACS Server/Database**<br>**Inadvertent or unauthorized access to or disclosure of FTC employee or contractor data** | To reduce privacy risks, employee profiles are created using only the minimum amount of PII necessary to verify and grant physical access to FTC facilities and other restricted areas. Access to the system is based on a valid access authorization and intended system use. All access is based on least-privilege and need-to-know security models. Data stored on backups is encrypted. |
| **NVR - Cameras**<br>**Collecting more information than is necessary** | 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 Physical Security Branch personnel and Security Guards have access to live video feeds and stored images. |
| **PACS Server/ Database and/or NVR** | This risk is reduced by the Office of the Chief Administrative Services Officer (OCASO) Chain of Custody and Evidence Storage policy and procedure, which establishes guidance |

**Loss of Exported**

### 8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

Security managers annually review the log of security employee access to PACS and may conduct other reviews more frequently, as needed. PIAs, including this one, are reviewed routinely to ensure accuracy. In addition, all FTC staff and contractors must review and