Federal Communications Commission

Office of the Managing Director

Privacy Impact Assessment[1] (PIA) for the Physical Access Control System (PACS)

September 26, 2008

FCC Bureau/Office: Office of the Managing Director, Administrative Operations (OMD-AO)
Division: Security Operations Center (SOC)

Privacy Analyst: Leslie F. Smith
Telephone Number: (202) 418-0217
E-mail Address: Leslie.Smith@fcc.gov

[1] This questionnaire is used to analyze the impacts on the privacy and security of the personally identifiable information (PII) that is being maintained in these records and files.

The *Privacy Act of 1974*, as amended, 5 U.S.C. 552a, requires Federal agencies to take special measures to protect personal information about individuals when the agencies collect, maintain, and use such personal information.

Having established through the **Privacy Threshold Assessment** that this information system contains information about individuals, *e.g.*, personally identifiable information (PII), it is important that when the FCC makes changes to such an information system, the FCC then analyzes:

(a) What changes are being made to the information that the system presently collects and maintains; and/or

(b) What new information will be collected and maintained to determine the continuing impact(s) on the privacy of the individuals.

The Privacy Impact Assessment template's purpose is to help the bureau/office to evaluate the changes in the information in the system and to make the appropriate determination(s) about how to treat this information, as required by the Privacy Act's regulations.

Section 1.0 Information System's Contents:

1.1 Status of the Information System:

☐ New information system—Development date:
☒ Revised or upgraded information system—Revision or upgrade date: September 2008

If this system is being revised—what will be done with the newly derived information:

☐ Placed in existing information system—Implementation Date:
☐ Placed in new auxiliary/ancillary information system—Date:
☐ Other use(s)—Implementation Date:

Please explain your response:

The PACS information system has been revised to conform to the requirements of Homeland Security Presidential Directive (HSPD) 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," (August 27, 2004) and associated guidance provided in OMB Memorandum M-06-06 (February 17, 2006). HSPD-12 required the FCC and other Federal agencies to have these requirements in effect on October 26, 2006. The FCC has made additional refinements to this information system in since then.

1.2 Has a Privacy Threshold Assessment been done?

☐ Yes
Date:
☒ No

If a Privacy Threshold Assessment has not been done, please explain why not:

This information system is covered by a system of records notice (SORN) that pre-dates the implementation of the Privacy Impact Assessment requirement.

If the Privacy Threshold Assessment (PTA) has been completed, please skip to Question 1.15

1.3 Has this information system, which contains information about individuals, *e.g.*, personally identifiable information (PII), existed under another name, *e.g.*, has the name been changed or modified?

☒ Yes
☐ No

If yes, please explain your response:

The system of records notice (SORN) that covers this information system was previously titled FCC/Central-10, "Access Control System." It was renamed and re-numbered FCC/OMD-24, "Physical Access Control System," SORN.

1.4 Has this information system undergone a "substantive change" in the system's format or operating system?

☒ Yes
☐ No

If yes, please explain your response:

The FCC has revised the PACS information system's operating systems to comply with the requirements of Homeland Security Presidential Directive 12 (HSPD-12) and made other revisions and refinements since October 2006.

If there have been no such changes, please skip to Question 1.7.

1.5 Has the medium in which the information system stores the records or data in the system changed from paper files to electronic medium (computer database); or from one electronic information system to another, *i.e.*, from one database, operating system, or software program, *etc.*?

☒ Yes
☐ No

If yes, please explain your response:

The FCC has revised the PACS information system's electronic information system technology to comply with the requirements of HSPD-12.

1.6 Has this information system operated as part of another information system or was it linked to another information system:

☐ Yes
☒ No

If yes, please explain your response:

The PACS information system's electronic databases are stored and maintained in the FCC's network computer information systems. There are no links or connections to computer information systems outside the FCC.

If the information system is not part of, nor linked to another information system, please skip to Question 1.8

1.7 Was it operated by another bureau/office or transferred from another Federal agency to the FCC?

☐ Yes
☐ No

Please explain your response:

1.8 What information is the system collecting, analyzing, managing, storing, transferring, *etc*:

Information about FCC Employees:

☐ No FCC employee information
☒ FCC employee's name
☒ Other names used, *i.e.*, maiden name, *etc*.
☒ FCC badge number (employee ID)
☐ SSN
☐ Race/Ethnicity
☐ Gender
☐ U.S. Citizenship
☐ Non-U.S. Citizenship
☒ Biometric data
  ☒ Fingerprints
  ☐ Voiceprints
  ☐ Retina scans/prints
  ☒ Photographs
  ☐ Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc*.:
☐ Birth date/age
☐ Place of birth
☐ Medical data
☐ Marital status
☐ Spousal information
☐ Miscellaneous family information:
☐ Home address
☐ Home address history
☐ Home telephone number(s)
☐ Personal cell phone number(s)
☐ Personal fax number(s)
☐ Personal e-mail address(es)
☐ Emergency contact data:
☐ Credit card number(s)
☐ Driver's license
☐ Bank account(s)
☐ FCC personal employment records
☐ Military records
☐ Financial history
☐ Foreign countries visited
☐ Law enforcement data:
☐ Background investigation history:
☐ National security data:
☐ Communications protected by legal privileges
☐ Signature:

☒ Other information: FCC organizational unit, *e.g.*, bureau/office, division, *etc.*, office/room number, and office telephone number; personal identify verification (PIV) card issue and expiration dates; computer access and permission rights; and parking permit information (as user applicable).

Information about FCC Contractors:

☐ No FCC contractor information
☒ Contractor's name
☐ Other name(s) used, *i.e.*, maiden name, *etc.*
☐ FCC Contractor badge number (Contractor ID)
☐ SSN
☐ Race/Ethnicity
☐ Gender
☐ U.S. Citizenship
☐ Non-U.S. Citizenship
☐ Biometric data
  ☒ Fingerprints
  ☐ Voiceprints
  ☐ Retina scans/prints
  ☒ Photographs
  ☐ Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc.*:
☐ Birth date/Age
☐ Place of birth
☐ Medical data
☐ Marital status
☐ Spousal information
☐ Miscellaneous family information
☐ Home address
☐ Home address history
☐ Home telephone number(s)
☐ Personal cell phone number(s)
☐ Personal fax number(s)
☐ Personal e-mail address(es)
☐ Emergency contact data:
☐ Credit card number(s)
☐ Driver's license number(s)
☐ Bank account(s)
☐ Non-FCC personal employment records
☐ Military records
☐ Financial history
☐ Foreign countries visited
☐ Law enforcement data
☐ Background investigation history:
☐ National security data:
☐ Communications protected by legal privileges
☒ Other information: Federal supervisor, supervisor's telephone number, contractor's office telephone number, FCC point of contact, FCC Bureau/Office, FCC office/room number, FCC telephone number; personal identify verification (PIV) card issue and expiration dates, PIV registrar approval signature; parking permit data; and computer access and permission rights.

Information about FCC Volunteers, Visitors, Customers, and other Individuals:

- ☐ Not applicable
- ☒ Individual's name
- ☐ Other name(s) used, *i.e.*, maiden name, *etc*.
- ☐ SSN
- ☐ Race/Ethnicity
- ☐ Gender
- ☐ Citizenship
- ☐ Non-U.S. Citizenship
- ☒ Biometric data
  - ☐ Fingerprints
  - ☐ Voiceprints
  - ☐ Retina scans/prints
  - ☒ Photographs
  - ☐ Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc*.
- ☐ Birth date/Age
- ☐ Place of birth
- ☐ Medical data
- ☐ Marital status
- ☐ Spousal information
- ☐ Miscellaneous family information
- ☐ Home address
- ☐ Home address history
- ☐ Home telephone number(s)
- ☐ Personal cell phone number(s)
- ☐ Personal fax number(s)
- ☐ Emergency contact data:
- ☐ Credit card number(s)
- ☐ Driver's license number(s)
- ☐ Bank account(s)
- ☐ Personal e-mail address(es)
- ☐ Non-FCC personal employment records
- ☐ Military records
- ☐ Financial history
- ☐ Foreign countries visited
- ☒ FCC Visitor badge number: Frequent visitor's badge number and issue and expiration dates; and Day contractor badge number and issue and expiration dates.
- ☐ Law enforcement data
- ☐ Background investigation history
- ☐ National security data
- ☐ Communications protected by legal privileges
- ☐ Digital signature
- ☒ Other information: Frequent visitor's employer's name and/or self-employment, telephone number, position, clearance type; FCC interns, volunteers, and individuals formerly in these positions; visitor's signature..

Information about Business Customers and others (usually not considered "personal information"):

- ☒ Not applicable
- ☐ Name of business contact/firm representative, customer, and/or others

- ☐ Race/Ethnicity
- ☐ Gender
- ☐ Full/Partial SSN
- ☐ Business/corporate purpose(s)
- ☐ Other business/employment/job description(s)
- ☐ Professional affiliations
- ☐ Business/office address
- ☐ Intra-business office address (office or workstation)
- ☐ Business telephone number(s)
- ☐ Business cell phone number(s)
- ☐ Business fax number(s)
- ☐ Business pager number(s)
- ☐ Business e-mail address(es)
- ☐ Bill payee name
- ☐ Bank routing number(s)
- ☐ Income/Assets
- ☐ Web navigation habits
- ☐ Commercially obtained credit history data
- ☐ Commercially obtained buying habits
- ☐ Credit card number(s)
- ☐ Bank account(s)
- ☐ Other information:

1.9 What are the sources for the information that you are collecting:

- ☒ Personal information from FCC employees: Personal data sufficient to satisfy the Physical Access Control System requirements.
- ☒ Personal information from FCC contractors: Personal data sufficient to satisfy the Physical Access Control System requirements.
- ☒ Personal information from non-FCC individuals and/or households: Personal data sufficient to satisfy the Physical Access Control System requirements.
- ☒ Non-personal information from businesses and other for-profit entities: Company name and/or self-employment.
- ☐ Non-personal information from institutions and other non-profit entities:
- ☐ Non-personal information from farms:
- ☐ Non-personal information from Federal Government agencies:
- ☐ Non-personal information from state, local, or tribal governments:
- ☐ Other sources:

1.10 Will the information system obtain, use, store, analyze, *etc*. information about individuals *e.g*, personally identifiable information (PII), from other information systems, including both FCC and non-FCC information systems?

- ☐ Yes
- ☒ No

Please explain your response:

If the information system does not use any PII from other information systems, please skip to Question 1.15

1.11 If the information system uses information about individuals from other information systems, what information will be used?

- ☐ FCC information system and/or non-FCC information system name(s):
- ☐ FCC employee's names:
- ☐ Non-FCC employee's names
- ☐ Other names uses, *i.e.*, maiden name, *etc*.
- ☐ FCC government badge number (employee ID)
- ☐ Non-FCC government badge number (contractor or other non-FCC employee ID)
- ☐ Citizenship:
- ☐ Biometric data
  - ☐ Fingerprints
  - ☐ Voiceprints
  - ☐ Retina scan/prints
  - ☐ Photographs
  - ☐ Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc*.
- ☐ Birth date/Age
- ☐ Place of birth
- ☐ Medical data
- ☐ Marital status
- ☐ Spousal information
- ☐ Miscellaneous family information:
- ☐ Home address
- ☐ Home address history
- ☐ Home telephone number(s)
- ☐ Personal cell phone number(s)
- ☐ Personal fax number(s)
- ☐ Emergency contact data
- ☐ Credit card number(s)
- ☐ Driver's license
- ☐ Bank account(s)
- ☐ Personal e-mail address(es)
- ☐ Non-FCC personal employment records
- ☐ Law enforcement data
- ☐ Military records
- ☐ National security data
- ☐ Communications protected by legal privileges
- ☐ Financial history
- ☐ Foreign countries visited
- ☐ Background investigation history
- ☐ Digital signature
- ☐ Other information:

Information about Business Customers and others (usually not considered "personal information"):

- ☐ Not applicable
- ☐ Name of business contact/firm representative, customer, and/or others
- ☐ Race/Ethnicity
- ☐ Gender
- ☐ Full/Partial SSN
- ☐ Business/corporate purpose(s)

☐ Other business/employment/job descriptions
☐ Professional affiliations
☐ Intra-business office address (office or workstation)
☐ Business telephone number(s)
☐ Business cell phone number(s)
☐ Business fax number(s)
☐ Business e-mail address(es)
☐ Bill payee name
☐ Bank routing number(s)
☐ Income/Assets
☐ Web navigation habits
☐ Commercially obtained credit history data
☐ Commercially obtained buying habits
☐ Personal clubs and affiliations
☐ Credit card number(s)
☐ Bank account(s)
☐ Other information:

1.12 Will this information system derive new information, records, or data, or create previously unavailable information, records, or data, through aggregation or consolidation from the information that will now be collected via this link to the other system, including information, records, or data, that are being shared or transferred from the other information system(s)?

☐ Yes
☐ No

Please explain your response:

1.13 Can the information, whether it is: (a) in the information system, (b) in a linked information system, and/or (c) transferred from another system, be retrieved by a name or a "unique identifier" linked to an individual, *e.g.*, SSN, name, home telephone number, fingerprint, voice print, *etc*.?

☐ Yes
☐ No

Please explain your response:

1.14 Will the new information include personal information about individuals, *e.g*., personally identifiable information (PII), be included in the individual's records or be used to make a determination about an individual?

☐ Yes
☐ No

Please explain your response:

1.15 Under the *Privacy Act of 1974*, as amended, 5 U.S.C. 552a, Federal agencies are required to have a System of Records Notice (SORN) for an information system like this one, which contains information about individuals, *e.g.*, "personally identifiable information" (PII).

A System of Records Notice (SORN) is a description of how the information system will collect, maintain, store, and use the personally identifiable information (PII).

Is there a SORN that already covers this PII in this information system?

☒ Yes
☐ No

If yes, what is this System of Records Notice (SORN): This SORN is titled FCC/OMD-24, "Physical Access Control System (PACS)."

Please provide the citation that was published in the *Federal Register* for the SORN: This SORN was published on September 25, 2006 (71 FR 55787, 55793).

If a SORN already covers this PII, please skip to **Section 2.0 System of Records Notice (SORN) Update** to address any changes to this SORN.

If a system of records notice (SORN) does not presently cover the information about individuals in this system, then it is necessary to determine whether a new FCC system of records notice must be created for the information.

1.16 If this information system is not covered by a system of records notice (SORN), does the information system exist by itself, or does it now, or did it previously exist as a component or subset of another SORN?

☐ Yes
☐ No

If yes, please explain what has occurred:

What is the System of Records Notice (SORN) of which it is currently or previously a component or subset:

Please also provide the citation that was published in the *Federal Register* for the SORN:

1.17 What are the purposes or functions that make it necessary to create a new a system of records notice (SORN) for this information system, *e.g.*, why is the information being collected?

1.18 Where is this information for the system of records notice (SORN) located?

1.19 Is the use of the information both relevant and necessary to the purposes for which the information system is designed, *e.g.*, is the SORN only collecting and using information for the specific purposes for which the SORN was designed so that there is no "extraneous" information included in the database(s) or paper files?

☐ Yes
☐ No

Please explain your response:

If the use of this information is both relevant and necessary to the processes for which this information system is designed, please skip to Question 1.21.

1.20 If not, why or for what reasons is the information being collected?

1.21 Is the information covered under a Security Classification as determined by the FCC Security Officer?

☐ Yes
☐ No

Please explain your response:

1.22 What is the legal authority that authorizes the development of the information system and the information/data collection?

1.23 In what instances would the information system's administrator/manager/developer permit disclosure to those groups outside the FCC for whom the information was not initially intended.

Such disclosures, which are referred to as "Routine Uses," are those instances that permit the FCC to disclose information from a SORN to specific "third parties." These disclosures may be for the following reasons:
(check all that are applicable)

☐ Adjudication and litigation:
☐ Committee communications:
☐ Compliance with welfare reform requirements:
☐ Congressional inquiries:
☐ Emergency response by medical personnel and law enforcement officials:
☐ Employment, security clearances, licensing, contracts, grants, and other benefits by the FCC:

☐ Employment, security clearances, licensing, contracts, grants, and other benefits upon a request from another Federal, state, local, tribal, or other public authority, *etc*.:
☐ FCC enforcement actions:
☐ Financial obligations under the Debt Collection Act:
☐ Financial obligations required by the National Finance Center:
☐ First responders, *e.g.*, law enforcement, DHS, FEMA, DOD, NTIA, *etc*.:
☐ Government-wide oversight by NARA, DOJ, and/or OMB:

☐ Labor relations (NTEU):
☐ Law enforcement and investigations:
☐ Program partners, e.g., WMATA, *etc*.:
☐ Breach of Federal data:
☐ Others "third party" disclosures:

1.24 Will the information be disclosed to consumer reporting agencies?
☐ Yes
☐ No

Please explain your response:

1.25 What are the policies for the maintenance and secure storage of the information?

1.26 How is information in this system retrieved?

1.27 What policies and/or guidelines are in place on how long the bureau/office will retain the information?

1.28 Once the information is obsolete or out-of-date, what policies and procedures have the system's managers/owners established for the destruction/purging of the data?

1.29 Have the records retention and disposition schedule(s) been issued or approved by the National Archives and Records Administration (NARA)?

☐ Yes
☐ No

Please explain your response:

If a NARA records retention and disposition schedule has been approved for this System of Records Notice (SORN), please skip to **Section 2.0 System of Records Notice (SORN) Update**:

1.30 If there is no NARA approved records retention and disposal schedule, has there been any coordination with the Performance Evaluation and Records Management Branch (PERM) or the Records Officer?

☐ Yes
☐ No

Please explain your response:

If this is a new System of Records Notice (SORN), please skip to **Section 3.0 Development, Management, and Deployment and/or Sharing of the Information:**

Section 2.0 System of Records Notice (SORN) Update:

If a System of Records Notice (SORN) currently covers the information, please provide information to update and/or revise the SORN:

2.1 Have there been any changes to the Security Classification for the information covered by the system of records notice (SORN) from what was originally determined by the FCC Security Officer?

☐ Yes
☒ No

Please explain your response:

FCC/OMD-24, "Personal Security Files," SORN has not received a security classification.

2.2 Have there been any changes to the location of the information covered by the system of records notice (SORN)?

☐ Yes
☒ No

Please explain your response:

The data in the information systems covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN is maintained in the FCC Security Operations Center (SOC) of the Administrative Operations Division of the Office of the Managing Director (OMD-AO).

2.3 Have there been any changes to the categories of individuals covered by the system of records notice (SORN)?

☒ Yes
☐ No

Please explain your response:

The FCC has revised the categories of records in the information system covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN to make them consistent with the requirements of Homeland Security Presidential Directive (HSPD) 12 and OMB guidance in Memorandum M-06-06 . These categories of individuals covered by this SORN include all individuals to whom the FCC has issued credentials, and who require regular, on-going access to FCC facilities and information technology systems. This includes, but is not limited to:

1. Current FCC employees and current contractors;
2. Frequent visitors, temporary hires, special parking access users, and day contractors;
3. Applicants for Federal employment or contract work;
4. FCC students, interns, volunteers, affiliates, and individuals formerly in these positions, *e.g.*, retired FCC employees; and
5. Non-FCC employees who are authorized to perform or to use services in FCC facilities on an on-going basis, *e.g.*, credit union employees, restaurant employees, and building maintenance and cleaning employee.

This system does apply to occasional visitors or to short-term guests to whom the FCC will issue temporary identification and credentials, and who may include:

1. All visitors to FCC, *e.g.*, non-FCC federal employees and contractors, students, interns, volunteers, and affiliates; and
2. Individuals authorized to perform or to use services provided in FCC facilities on an infrequent basis, *e.g.*, and service and maintenance workers performing cleaning, maintenance, and repair duties in the Commission's buildings and facilities.

2.4 Have there been any changes to the categories of records, *e.g.*, types of information (or records) that the system of records notice (SORN) collects, maintains, and uses?

☒ Yes
☐ No

Please explain your response:

The FCC has revised the categories of records in the information system covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN to make them consistent with the requirements of Homeland Security Presidential Directive (HSPD) 12 and OMB guidance in Memorandum M-06-06. The SORN consists of a computer database containing the records of those individuals to whom the FCC has issued credentials. The records are filed alphabetically by last name, with a corresponding badge number, and include the following:

1. FCC employee/temporary hire database includes: First and last names, image (photograph), FCC telephone number, FCC Bureau/Office, FCC office/room number, personal identify verification (PIV) card issue and expiration dates, parking permit data, and computer system user access and permission rights.
2. Contractor database includes: First and last names, image (photograph), fingerprints, FCC point of contact, FCC telephone number, and FCC contractor badge number, personal identify verification (PIV) card and issue and expiration dates.
3. Frequent Visitor's database includes: First and last names, employer's name and/or self-employment, employer's address, employer's telephone number, position, (security) clearance type, image (photograph), and ID badge's issue and expiration dates.
4. Day contractor database includes: First and last name along with, badge number, issue and expiration dates.
5. Visitor database includes: First and last name, image (photograph) (future), FCC point of contact, signature, and issue date.
6. Special Parking Access database includes: First and last name, telephone number, employer, FCC point of contact, and issue date.

Note: Records maintained on cardholders entering FCC facilities or using FCC systems, *e.g.*, FCC employees and contractors, include: Individual's first, middle, and last name, PIV card number, date, time, and location of entry and exit, FCC bureau/office, contractor/visitor's employer's name, address, telephone number, level of national security clearance and expiration date, digital signature information, and computer networks/applications/data accessed, and FCC point of contact.

2.5 Have there been any changes to the legal authority under which the FCC collects and maintains the information covered by the system of records notice (SORN)?

☒ Yes
☐ No

Please explain your response:

The FCC has revised the authority for maintenance of the records in the information system covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN to make it consistent with the requirements of Homeland Security Presidential Directive 12 (HSPD-12) and OMB guidance in Memorandum M-06-06, and which include 5 U.S.C. 301; Federal Information Security Act (Pub. L. 104–106, sec. 5113); Electronic Government Act (Pub. L. 104–347, sec. 203); Paperwork Reduction Act of 1995 (44 U.S.C. 3501); Government Paperwork Elimination Act (Pub. L. 105–277, 44 U.S.C. 3504); Homeland Security Presidential Directive (HSPD) 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004; Federal Property and Administrative Act of 1949, as amended; and Department of Justice Report, "Vulnerability Assessment of Federal Facilities," June 28, 1995.

2.6 Have there been any changes to the purposes for collecting, maintaining, and using the information covered by the system of records notice (SORN)?

☐ Yes
☒ No

Please explain your response:

The FCC has revised the purposes for collecting, maintaining, and using the records in the information system covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN to comply with HSPD-12 and OMD guidance in Memorandum M-06-06, as follows:

1. To ensure the safety and security of FCC facilities, systems, and information, FCC employees, contractors, interns, guests, and frequent visitors;
2. To verify that all people entering the FCC facilities, using FCC and Federal information resources (or accessing classified information), are authorized to do so;
3. To track and control FCC badges (PIV cards) issued to individuals entering and exiting these facilities, using FCC systems, or accessing classified information; and
4. To provide a method by which the FCC may ascertain the times each person was in these facilities.

2.7 Have there been any changes to the Routine Uses under which disclosures are permitted to "third parties" as noted in the system of records notice (SORN)?

☒ Yes
☐ No

Please check all Routine Uses that apply and provide any explanation as required:

☒ Adjudication and litigation:
☐ Committee communications:
☐ Compliance with welfare reform requirements:
☒ Congressional inquiries:
☒ Contract Services, grants, or cooperative agreements:
☐ Emergency response by medical personnel and law enforcement officials:

☒ Employment, security clearances, licensing, contracts, grants, and other benefits by the FCC:

☒ Employment, security clearances, licensing, contracts, grants, and other benefits upon a request from another Federal, state, local, tribal, or other public authority, *etc.*:
☐ FCC enforcement actions:
☐ Financial obligations under the Debt Collection Act:
☐ Financial obligations required by the National Finance Center:
☐ First responders, *e.g.*, law enforcement, DHS, FEMA, DOD, NTIA, *etc*.:
☒ Government-wide program management and oversight by NARA, DOJ, and/or OMB:
☒ Labor relations: Note that disclosures to the FCC of data pertaining to date and time of entry and exit of a Commission employee working in the District of Columbia may not be made to supervisors, managers, or any other individuals (other than the individual to whom the information applies) to verify the employee's time and attendance record for personnel actions because 5 U.S.C. 6106 prohibits Federal Executive Agencies (other than the Bureau of Engraving and Printing) from using a recording clock within the District of Columbia, unless the clock is used as part of a flexible schedule program under 5 U.S.C. 6120 *et seq*.
☐ Law enforcement and investigations:
☒ Department of Justice (DOJ):
☒ National security and intelligence matters:
☐ Program partners, *e.g.*, WMATA:
☒ Breach of Federal data: Required by OMB Memorandum M-07-16 (May 22, 2007).
☒ Others Routine Use disclosures not listed above: Invalid PIV card notfication--disclosure may be made to notify another Federal agency, when, or to verify whether, a PIV card is not longer valid.

2.8 Have there been any changes as to whether the FCC will permit the information covered by the system of records notice (SORN) to be disclosed to consumer reporting agencies?

☐ Yes
☒ No

Please explain your response:

The FCC does not permit information in FCC/OMD-24, "Physical Access Control System (PACS)," SORN to be disclosed to consumer reporting agencies.

2.9 Have there been any changes to the policies and/or guidelines for the storage and maintenance of the information covered by this system of records notice (SORN)?

☒ Yes
☐ No

Please explain your response:

The data in the information systems covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN are maintained in paper files, which are stored in file folders in locked file cabinets, and in electronic records, which are stored in password-protected or logical access controlled electronic media, *e.g.*, computer database(s) on the FCC's network computer database. There are no links to any computer networks outside the FCC.

2.10 Have there been any changes to how the information covered by the system of records notice (SORN) is retrieved or otherwise accessed?

☒ Yes
☐ No

Please explain your response:

The FCC has revised the retrieval and access procedures for the information system that is covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN to comply with the requirements of HSPD-12 and OMB guidelines in Memorandum M-06-06 (February 17, 2006). Information can be retrieved by:

(1) the name of the individual;

(2) other ID number, *e.g.*, FCC employee, contractor, or frequent visitor badge number; or

(3) PIV card serial number.

2.11 Have there been any changes to the safeguards that the system manager has in place to protect unauthorized access to the information covered by the system of records notice (SORN)?

☒ Yes
☐ No

Please explain your response:

FCC/OMD-24, "Physical Access Control System (PACS)" SORN includes paper files and electronic records. The safeguards that the system manager has in place to protect unauthorized access to the information covered by the system of records notice (SORN) comply with the requirements of HSPD-12, OMB guidelines in Memorandum M-06-06 (February 17, 2006),and FIPS 201, as follows:

Paper records are kept in locked cabinets in secure facilities and access to them is restricted to individuals, *e.g.*, FCC Security Operations Center staff, whose duties and responsibilities require their use of the information.

The computer servers in which the information is stored are located in FCC facilities that are secured by limited access card readers. The computer servers themselves are password-protected. Access by individuals working at guard stations is password-protected; each person granted access to the system at guard stations must be individually authorized to use the system. A *Privacy Act Warning Notice* appears on the monitor screen when records containing information on individuals are first displayed. The staff in the FCC's Information Technology Division (IT) in the Office of Managing Director (OMD-IT) performs a backup operation on these files on a regular basis using a secure medium. The backup data are stored in a locked and controlled room in a secure location.

Please note that you must also provide an update of the current protections, safeguard, and other security measures that are in place in this SORN in **Section 5.0 Safety and Security Requirements:**

2.12 Have there been any changes to the records retention and disposition schedule for the information covered by the system of records notice (SORN)? If so, has the system manager worked with the Performance Evaluation and Records Management (PERM) staff to insure that this revised schedule been approved by the National Archives and Records Administration (NARA)?

☐ Yes
☒ No

Please explain your response:

The PERM staff has reviewed FCC/OMD-24, "Physical Access Control System (PACS)," SORN and has determined that the records relating to individuals with FCC access cards, covered by this system, are retained in accordance with General Records Schedule 18, Item 17 approved by the National Archives and Records Administration (NARA). The records disposal is done in accordance with the Commission's disposal policies. Unless retained for specific, on-going security investigations, records of facility access are maintained for one year and then destroyed.

All other records relating to individuals are retained and disposed of in accordance with General Records Schedule 18, item 22a, approved by NARA. The records are disposed of in accordance with FCC Security Operations Center disposal policies, as follows:

1. When an employee/contractor/temporary hire/special parking access leaves the FCC, the file in the database is deleted.
2. Frequent visitor badges are given a two-year valid period, after which the card will automatically deactivate.
3. All returned day contractor cards will be reused on a daily basis.
4. Transaction data for all cards will be stored using a secure medium and retained for one year in the FCC Security Operations Center, which is locked and secured with an alarm system. Otherwise, access records are destroyed upon notification of death, or not later than one year after the employee's retirement or separation from the FCC, or the employee's transfer to another Federal agency, whichever is applicable.

In accordance with HSPD-12, PIV Cards are deactivated within eighteen (18) hours of notification of cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with General Records Schedule 11, Item 4. PIV Cards are destroyed by burning in an approved Federal burn-facility.

The NARA Schedule 18 may be viewed at: *http://www.archives.gov/records-mgmt/ardor/grs18.html.*

Section 3.0 Development, Management, and Deployment and/or Sharing of the Information:

3.1 Who will develop the information system(s) covered by this system of records notice (SORN)?

☐ Developed wholly by FCC staff employees:
☐ Developed wholly by FCC contractors:
☒ Developed jointly by FCC employees and contractors:
☐ Developed offsite primarily by non-FCC staff:
☐ COTS (commercial-off-the-shelf-software) package:
☒ Other development, management, and deployment/sharing information arrangements: The PIV system includes "turn key" system components for which the FCC and the IT contracting staff will determine the data fields that are used at FCC headquarters, Gettysburg, PA, and Laurel, MD.

3.2 Where will the information system be hosted?

☒ FCC Headquarters:
☐ Gettysburg
☐ San Diego
☐ Colorado
☐ New York

☐ Columbia Lab
☐ Chicago
☐ Other information:

3.3 Who will be the primary manager(s) of the information system who will be responsible for assuring access to, proper use of, and protecting the security and integrity of the information? (Check all that apply and provide a brief explanation)

☒ FCC staff in this bureau/office exclusively: FCC Security Operations Center staff in the Administrative Operations Division of the Office of the Managing Director (OMD-AO) has responsibility for access and proper use of the information on a "need-to-know" basis.
☐ FCC staff in other bureaus/offices:
☐ Information system administrator/Information system developers:
☐ Contractors:
☐ Other information system developers, *etc*:

3.4 What are the FCC's policies and procedures that the information system administrators and managers use to determine who gets access to the information in the system's files and/or database(s)?

The information system administrators and managers make a determination about which FCC employees are granted access the information in FCC/OMD-24, "Physical Access Control System (PACS)," SORN on a "need to know" basis, as determined by the job duties and responsibilities of the FCC employee in the FCC's Security Operations Center and/or IT contractor.

3.5 How much access will users have to data in the information system(s)?

☐ Access to all data:
☒ Restricted access to data, as determined by the information system manager, administrator, and/or developer: The FCC Security Operations Center staff will determine who is granted access.
☐ Other access policy:

3.6 Based on the Commission policies and procedures, which user group(s) may have access to the information at the FCC:–
(Check all that apply and provide a brief explanation)

☐ Information system managers:
☒ Information system administrators: Staff in the FCC's Information Technology Divisions of the Office of the Managing Director (OMD-IT), that includes the IT system administrators– both FCC employees and contractors who manage the IT information systems.
☐ Information system developers:
☒ FCC staff in this bureau/office: FCC's Security Operations Center grants access based on a "need to know" basis.
☐ FCC staff in other bureaus/offices:
☐ FCC staff in other bureaus/offices in FCC field offices:
☒ Contractors: IT contractors working at the FCC are granted access based on a "need to know" basis.
☐ Other Federal agencies:
☐ State and/or local agencies:
☐ Businesses, institutions, and other groups:
☐ International agencies:
☐ Individuals/general public:

☐ Other groups:

3.7 If contractors are part of the staff in the FCC who collect, maintain, and access the information, does the IT supervisory staff ensure that contractors adhere fully to the Privacy Act provisions, as required under subsection (m) of the Privacy Act, as amended, 5 U.S.C. 552a(m)?

☒ Yes
☐ No

Please explain your response:

The FCC's Security Operations Center supervisory staff provide periodic privacy training to the FCC's employees and IT contractors who manage the information system's computer databases.

3.8 Has the Office of the General Counsel (OGC) signed off on any Section M contract(s) for any contractors who work with the information system covered by this system of records notice (SORN)?

☒ Yes
☐ No

Please explain your response:

The contacts that cover the IT contractors who manage the data in this information system covered by FCC/OMD-24, "Physical Access Control System," SORN include a requirement that they abide by Section M of the Privacy Act, 5 U.S.C. 552a(m).

3.9 Does the information system covered by this system of records noticed (SORN) transmit/share personal information, *e.g.*, personally identifiable information (PII), between the FCC information technology (IT) network(s) and a public or other non-FCC IT network(s), which are not covered by this Privacy Impact Assessment?

☐ Yes
☒ No

Please explain your response:

The electronic data in the information system covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN are stored in the FCC's computer networks. No data in electronic format are transmitted outside the FCC's computer network system, nor are the paper files shared or otherwise made available for use outside the FCC, except as stated in the Routine Uses.

If there is no information sharing or transmission, please skip to **Section 4.0 Data Quality, Utility, Objectivity, and Integrity Requirements:**

3.10 If the information system covered by this system of records noticed (SORN) transmits/shares personal information between the FCC network and a public or other non-FCC network, which is not covered by this Privacy Impact Assessment, what information is shared/transmitted/disclosed and for what purposes?

3.11 If there is such transmission/sharing of personal information, how is the information secured for transmission—what security measures are used to prevent unauthorized access during transmission, *i.e.*, encryption, *etc.*?

3.12 If there is sharing or transmission to other information systems, with what other non-FCC organizations, groups, and individuals will the information be shared?
(Check all that apply and provide a brief explanation)

☐ Other Federal agencies:
☐ State, local, or other government agencies:
☐ Businesses:
☐ Institutions:
☐ Individuals:
☐ Other groups:

If there is no "matching agreement," *e.g., Memorandum of Understand (MOU), etc.*, please skip to **Section 4.0 Data Quality, Utility, Objectivity, and Integrity Requirements:**

3.13 What kind of "matching agreement," *e.g., Memorandum of Understanding (MOU), etc.*, as defined by 5 U.S.C. 552a(u) of the Privacy Act, as amended, is there to cover the information sharing and/or transferal with the external organizations?

3.14 Is this a new or a renewed matching agreement?

☐ New matching agreement
☐ Revised matching agreement

Please explain your response:

3.15 Has the matching agreement been reviewed and approved (or renewed) by the FCC's Data Integrity Board, which has administrative oversight for all FCC matching agreements?

☐ Yes
If yes, on what date was the agreement approved:
☐ No

Please explain your response:

3.17 How is the information that is covered by this system of records notice (SORN) transmitted or disclosed with the external organization(s) under the *MOU* or other "matching agreement?"

3.18 How is the shared information secured by the recipient under the *MOU*, or other "matching agreement?"

Section 4.0 Data Quality, Utility, Objectivity, and Integrity Requirements:

OMB regulations require Federal agencies to insure that the information/data that they collect and use meets the highest possible level of quality and integrity. It is important, therefore, that the information the Commission's information systems use meets the "benchmark standards" established for the information.

4.1 How will the information that is collected from FCC sources, including FCC employees and contractors, be checked for accuracy and adherence to the Data Quality guidelines? (Please check all that apply)

☒ Information is processed and maintained only for the purposes for which it is collected.
☒ Information is reliable for its intended use(s).
☒ Information is accurate.
☒ Information is complete.
☒ Information is current.
☐ Not applicable:

Please explain any exceptions or clarifications:

The information that is covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN and is contained in its paper files and electronic databases includes personal identifiable (background) information (PII) that the FCC is required to gather and maintain as required by Homeland Presidential Directive (HSPD) 12 and OMD Memorandum M-06-06 (February 17, 2006). HSPD-12 also includes regulations to insure that the information that the FCC and other Federal agencies gather and maintain is accurate and adheres to the Data Quality guidelines. The PII covers any individual who requires regular, on-going access to FCC facilities and information technology systems. This includes but is not limited to:

1. Current FCC employees and current contractors;

2. Frequent visitors, temporary hires, special parking access users, and day contractors;
3. Applicants for Federal employment or contract work;

4. FCC students, interns, volunteers, affiliates, and individuals formerly in these positions, e.g., retired FCC employees; and

5. Non-FCC employees who are authorized to perform or use services in FCC facilities on an on-going basis, *e.g.*, credit union employees, restaurant employees, and building maintenance and cleaning employee.

This system does apply to occasional visitors or short-term guests to whom the FCC will issue temporary identification and credentials, who may include:

1. All visitors to FCC, *e.g.*, non-FCC federal employees and contractors, students, interns, volunteers, and affiliates; and

2. Individuals authorized to perform or use services provided in FCC facilities on an infrequent basis, *e.g.*, and service and maintenance workers performing cleaning, maintenance, and repair duties in the Commission's buildings and facilities.

If the Data Quality Guidelines do not apply to the information in this information system, please skip to **Section 5.0 Safety and Security Requirements:**

4.2 Is any information collected from non-FCC sources; if so, how will the information sources be checked for accuracy and adherence to the Data Quality guidelines?
(Please check all that apply and provide an explanation)

☒ Yes, information is collected from non-FCC sources:
- ☒ Information is processed and maintained only for the purposes for which it is collected:
- ☒ Information is reliable for its intended use(s):
- ☒ Information is accurate:
- ☒ Information is complete:
- ☒ Information is current:

☐ No information comes from non-FCC sources:

Please explain any exceptions or clarifications:

The information that is covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN and is contained in its paper files and electronic databases includes personal identifiable (background) information (PII) that the FCC is required to gather and maintain as required by Homeland Presidential Directive (HSPD) 12 and OMD Memorandum M-06-06 (February 17, 2006). HSPD-12 also includes regulations to insure that the information that the FCC and other Federal agencies gather and maintain is accurate and adheres to the Data Quality guidelines. The PII covers any individual who requires regular, on-going access to FCC facilities and information technology systems. This includes but is not limited to:

1. Current FCC employees and current contractors;

2. Frequent visitors, temporary hires, special parking access users, and day contractors;
3. Applicants for Federal employment or contract work;

4. FCC students, interns, volunteers, affiliates, and individuals formerly in these positions, e.g., retired FCC employees; and

5. Non-FCC employees who are authorized to perform or use services in FCC facilities on an on-going basis, *e.g.*, credit union employees, restaurant employees, and building maintenance and cleaning employee.

This system does apply to occasional visitors or short-term guests to whom the FCC will issue temporary identification and credentials, who may include:

1. All visitors to FCC, *e.g.*, non-FCC federal employees and contractors, students, interns, volunteers, and affiliates; and

2. Individuals authorized to perform or use services provided in FCC facilities on an infrequent basis, *e.g.*, and service and maintenance workers performing cleaning, maintenance, and repair duties in the Commission's buildings and facilities.

If the information that is covered by this system of records notice (SORN) is not being aggregated or consolidated, please skip to Question 4.5.

4.3 If the information that is covered by this system of records notice (SORN) is being aggregated or consolidated, what controls are in place to insure that the information is relevant, accurate, and complete?

Homeland Presidential Directive (HSPD) 12 regulations and OMB guidance in Memorandum M-06-06 (February 17, 2006) require the FCC and other Federal agencies to insure that the personally identifiable information (PII) that they gather and maintain on individuals is relevant, accurate, and complete and that it adheres to the Data Quality guidelines in those instances and circumstances when it is aggregated or consolidated by the FCC.

4.4. What policies and procedures do the information system's administrators and managers use to insure that the information adheres to the Data Quality guidelines both when the information is obtained from its sources and when the information is aggregated or consolidated for the use by the bureaus and offices?

The staff in the FCC's Security Operations Center follow the HSPD-12 regulations and OMB guidance in Memorandum M-06-06 (February 17, 2006) when the PII information, including both paper files and electronic data, in the information system covered by FCC/OMD-24, "Physical Access Control System (PACS)," SOR, is obtained from their sources and when the information is aggregated or consolidated for use by the FCC's bureaus and offices. Such scrupulous compliance insures that the Data Quality guidelines are always met with regards to this PII.

4.5 How often are the policies and procedures checked routinely—what type of annual verification schedule has been established to insure that the information that is covered by this system of records notice adheres to the Data Quality guidelines?

The FCC's Security Operations Center staff conducts an annual verification to insure that the PII information that is maintained in the information systems, which is covered by FCC/OMD-24, "Physical Access Control System," SORN, adheres to the Data Quality Guidelines.

Section 5.0 Safety and Security Requirements:

5.1 How are the records/information/data in the information system covered by this system of records notice (SORN) stored and maintained?

☒ IT database management system (DBMS)
☐ Storage media including diskettes, CDs, CD-ROMs, *etc*.
☐ Electronic tape
☒ Paper files
☐ Other:

5.2 Is the information collected, stored, analyzed, or maintained by this information system available in another form or from another source (other than a "matching agreement" or *MOU*, as noted above)?

☒ Yes
☐ No

Please explain your response:

The FCC is part of the General Services Administration's "shared services agreement" consortium of small Federal agencies.

5.3 Is the information system covered by this system of records notice (SORN) part of another FCC information system that collects personally identifiable information (PII)?

☐ Yes
☒ No

Please explain your response:

The paper files and electronic data in this information system are covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN.

If this information system is not part of another FCC information system, please skip to Question 5.7.

5.4 If the information system (under review here) has personally identifiable information (PII) and is part of another FCC information system, is there a transfer of records/data/information between these two FCC information system(s)?

☐ Yes
☒ No

Please explain your response:

There is not information transferred between the Physical Access Control System (PACS) and other FCC information systems in the FCC information technology network.

5.5 If the information system's personally identifiable information (PII) is part of another FCC information system, does the information system have processes and/or applications that are part of those from the other FCC information systems?

☐ Yes
☒ No

Please explain your response:

The Physical Access Control System (PACS) does not interact with other FCC information systems in the FCC's information technology network.

5.6 If either or both such situations, as noted in Questions 5.4 and 5.5 exist, what security controls are there to protect the PII information and to prevent unauthorized access?

☒ Not applicable.

Please explain your response:

5.7 Would the unavailability of this information system prevent the timely performance of FCC operations?

☒ Yes
☐ No

Please explain your response:

The information covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN is required under HSPD-12 and OMB guidelines in Memorandum M-06-06. Without the ability to gather, to analyze, and to maintain this personally identifiable information (PII), the FCC could not determine the background of the individuals to whom it grants access to its buildings, facilities, and information technology services, *e.g.*, that the FCC needs the ability to insure that

those who are hired as Federal employees, contractors who work at the FCC, and others who are authorized to gain access to and/or to perform or to use services provided in FCC facilities, and those who require regular on-going access to FCC and other Federal facilities, information technology, *etc*., those who are temporary or short-term employees, *i.e.*, instructors, consultants, and visitor, and those who are or were involved in Federal programs such as students and interns, *etc.*, meet the necessary security clearances for access to these FCC and other Federal buildings, facilities, and services.

5.8 Will the information system include an externally facing information system or portal such as an Internet accessible web application at www.fcc.gov that allows customers/users to access development, production, or internal FCC networks, and which may pose potential risks to the information's security?

☐ Yes
☒ No

Please explain your response:

The FCC's employment application process includes an externally facing information portal at www.fcc.gov through which applicants for FCC job openings may submit their Federal employment application form(s) and accompanying documentation.

5.9 Is the information is collected via www.fcc.gov or other URL from the individuals, how does the information system notify users about the Privacy Notice; if not applicable, please skip to Question 5.12:

☒ Link to the FCC's privacy policies for all users:
☐ Privacy notice displayed on the webpage:
☒ Privacy notice printed at the form or document: Federal job applications and related forms, *etc.*
☐ Website uses another method to alert users to the Privacy Act Notice, as follows:
☐ If there is no link or notice, why not:

5.10 If a privacy notice is displayed, which of the following are included?

☒ Proximity and timing—the privacy notice is provided at the time and point of data collection.
☒ Purpose—describes the principal purpose(s) for which the information will be used.
☒ Authority—specifies the legal authority that allows the information to be collected.
☒ Conditions—specifies whether providing the information is voluntary, and the effects, if any, of not providing it.
☒ Disclosures—specifies the routine use(s) that may be made of the information.
☐ Not applicable, as information will not be collected in any other way.

Please explain your response:

5.11 Will the information system include another customer-facing web site not on www.fcc.gov?

☐ Yes
☒ No

Please explain your response:

5.12 If the information system has a customer-facing web site via the FCC Intranet for FCC employees and contractors working at the FCC, does this web site(s) have a Privacy Act Notice and how is it displayed? If not applicable, please skip to Question 5.14.

☐ Yes
- ☐ Notice is displayed prominently on this FCC Intranet website:
- ☐ Link is provided to a general FCC Privacy Notice for all users:
- ☐ Privacy Notice is printed at the end of the form or document:
- ☐ Website uses another method to alert users to the Privacy Act Notice:

☒ No

If there is no Privacy Act Notice, please explain why not:

5.13 If a privacy notice is displayed, which of the following information is included?

☐ Proximity and timing—the privacy notice is provided at the time and point of data collection.
☐ Purpose—describes the principal purpose(s) for which the information will be used.
☐ Authority—specifies the legal authority that allows the information to be collected.
☐ Conditions—specifies if providing the information is voluntary, and the effects, if any, of not providing it.
☐ Disclosures—specifies the routine use(s) that may be made of the information.
☐ Not applicable, as information will not be collected in any other way.

Please explain your response:

5.14 If information is collected from the individual by fax, e-mail, FCC form(s), or regular mail, how is the privacy notice provided; if not applicable, please skip to Question 5.16?

☒ Privacy notice is on the document, *e.g.*, FCC form, *etc*.: FCC Form A-600, FCC Frequent Visitor Badge Form, FCC Employee Identification Badge Form, FCC Contractor Identification Badge Form, and FCC Visitors Sign-in Sheet.
☐ Privacy notice displayed on the webpage where the document is located:
☐ Statement on the document notifies the recipient that they may read the FCC Privacy Notice at http://www.fcc.gov/fccprivacypolicy.html.
☐ Website or FCC document uses other method(s) to alert users to the Privacy Act Notice:

☐ Privacy notice is provided via a recorded message or given verbally by the FCC staff handling telephone calls:
☒ No link or notice, please explain why not: The FCC gathers the personal contact information from the participating organizations, *i.e.*, Federal agencies, as required under HSPD-12 and OMB guidance in Memorandum M-06-06.
☐ Not applicable, as personally identifiable information (PII) will not be collected.

5.15 If a privacy notice is displayed, which of the following information is included?

☒ Proximity and timing—the privacy notice is provided at the time and point of data collection.
☒ Purpose—describes the principal purpose(s) for which the information will be used.
☒ Authority—specifies the legal authority that allows the information to be collected.
☒ Conditions—specifies if providing the information is voluntary, and the effects, if any, of not providing it.
☒ Disclosures—specifies the routine use(s) that may be made of the information.

☐ Not applicable, as information will not be collected in any other way.

Please explain your response:

If there is no access to the information system from outside the FCC via www.FCC.gov or other URL, please skip to Question 5.17.

5.16 If consumers may access the information and/or the information system on-line via www.FCC.gov, does it identify ages or is it directed to people under 13 years old?

☐ Yes
☒ No

Please explain your response:

Individuals applying for employment at the FCC via www.FCC.gov would be older than 13 years of age.

5.17 Will the FCC use the newly obtained information or revised information found in the information system covered by the existing system of records notice (SORN) to make a determination about the individual?

☐ Yes
☒ No

Please explain your response:

The HSPD-12 regulations and OMB guidance in Memorandum M-06-06 (February 17, 2006) require the FCC's Security Operations Center to use the personally identifiable information (PII) in this information system, including data obtained from paper files and electronic records data, for the following reasons:

1. To ensure the safety and security of FCC facilities, systems, and information, FCC employees, contractors, interns, guests, and frequent visitors;
2. To verify that all people entering the FCC facilities, using FCC and Federal information resources (or accessing classified information), are authorized to do so;
3. To track and control FCC badges (PIV cards) issued to individuals entering and exiting these facilities, using FCC systems, or accessing classified information; and
4. To provide a method by which the FCC may ascertain the times each person was in these facilities.

All the uses of the information, as enumerated above, that are collected from both FCC and non-FCC sources and are maintained by this information system are covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN.

5.18 Do individuals have the right to decline to provide personally identifiable information (PII)?

☐ Yes
☒ No

Please explain your response:

Individuals may not decline to provide the personally identifiable information (PII), which the FCC collects as part of its responsibilities under HSPD-12, OMB guidance in Memorandum M-06-06 (February 17, 2006), and other Federal employment regulations, *e.g.*, OPM requirements.

Failure to comply with these requirements is likely to terminate the job application process or prevent the individual from gaining access to the FCC and other Federal buildings, facilities, and services.

5.19 Do individuals have the right to consent to particular uses of their personal information?

☐ Yes
☒ No

Please explain your response:

Individuals do not have the right to consent to particular uses of their personally identifiable information (PII), which the FCC will collects as part of its responsibilities under HSPD-12, OMD guidance in Memorandum M-06-06, and other Federal employment regulations. By signing the employment or background review document, the individual gives his/her consent. Failure to consent is likely to terminate any job application process or prevent the individual from gaining access to the FCC's buildings, facilities, and services.

If individuals do <u>not</u> have the right to consent to the use of their information, please skip to Question 5.23.

5.20 If individuals have the right to consent to the use of their personal information, how does the individual exercise this right?

5.21 What processes are used to notify and to obtain consent from the individuals whose personal information is being collected?

5.22 What kinds of report(s) can the information system and/or the information be used to produce on the individuals whose PII data are in the information system covered by the system of records notice (SORN)?

The FCC uses the information, including that obtained from paper files and electronic records, and which is covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN to determine whether an individual should be granted access to FCC and other Federal buildings, facilities, and information technology services, *etc.*

5.23 What safeguards and security measures, including physical and technical access controls, are in place to secure the information and to minimize unauthorized access, use, or dissemination of the information that is stored and maintained in the information system?
(Check all that apply)

☒ Account name
☒ Passwords
  ☐ Accounts are locked after a set period of inactivity
  ☒ Passwords have security features to prevent unauthorized disclosure, *e.g.*, "hacking"
  ☐ Accounts are locked after a set number of incorrect attempts
  ☐ One time password token
  ☐ Other security features:
☒ Firewall
☐ Virtual private network (VPN)
☐ Data encryption

- ☒ Intrusion detection application (IDS)
- ☒ Common access cards (CAC)
- ☐ Smart cards
- ☒ Biometrics: FCC ID Badge has wearer's photograph.
- ☐ Public key infrastructure (PKI)
- ☒ Locked file cabinets or fireproof safes
- ☒ Locked rooms, with restricted access when not in use
- ☐ Locked rooms, without restricted access
- ☒ Documents physically marked as “sensitive”
- ☒ Guards
  - ☒ Identification badges
  - ☒ Key cards
  - ☒ Cipher locks
  - ☒ Closed circuit TV (CCTV)
  - ☐ Other:

5.24 Please explain what staff security training and other measures are in place to assure that the security and privacy safeguards are maintained adequately?

All FCC employees and contractors who work with the information system covered by FCC/OMD-24, “Physical Access Control System (PACS),” SORN are required to complete privacy training. In addition the Security Operations Center (SOC) staff emphasizes to those with access that this information is not to be shared or disclosed without prior authorization.

5.25 How often are security controls reviewed?

- ☒ Six months or less: The FCC's Security Operations Center staff reviews the security controls on a daily basis.
- ☐ One year
- ☐ Two years
- ☐ Three years
- ☐ Four years
- ☐ Five years
- ☐ Other:

5.26 How often are personnel (information system administrators, users, information system/information system developers, contractors, *etc*.) who use the information system trained and made aware of their responsibilities for protecting the information?

- ☐ There is no training
- ☒ One year: The FCC's Security Operations Center conducts privacy training for its staff on an annual basis, in addition to any Commission-wide training that is required for FCC employees and contractors.
- ☐ Two years
- ☐ Three years
- ☐ Four years
- ☐ Five years
- ☒ Other: The FCC has also inaugerated a Commission-wide privacy training program, and all employees and contractors were required to complete the privacy training course in September 2006.

If privacy training is provided, please skip to Question 5.28.

5.27 What are the safeguards to insure that there are few opportunities for disclosure, unavailability, modification, and/or damage to the information system covered by this system of records notice (SORN), and/or prevention of timely performance of FCC operations if operational training is not provided?

5.28 How often must staff be "re-certified" that they understand the risks when working with personally identifiable information (PII)?

☒ Less than one year: The FCC's Security Operations Center reviews security controls on a daily basis.
☐ One year
☐ Two years
☐ Three or more years
☐ Other re-certification procedures:

5.29 Do the Commission's training and security requirements for this information system that is covered by this system of records notice (SORN) conform to the requirements of the Federal Information Security Management Act (FISMA)?

☒ Yes
☐ No

Please explain your response:

The FCC/OMD-24, "Physical Access Control System (PACS)," SORN and all its procedures covering the personally identifiable information (PII) conform to FISMA requirements, as required by HSPD-12 and OMB regulations in Memorandum M-06-06 (February 17, 2006).

If the Privacy Threshold Assessment was completed recently as part of the information system's evaluation, please skip to Question 5.34.

5.30 What is the potential impact on individuals on whom the information is maintained in the information system(s) if unauthorized disclosure or misuse of information occurs? (check one)

☐ Results in little or no harm, embarrassment, inconvenience, or unfairness to the individual.
☐ Results in moderate harm, embarrassment, inconvenience, or unfairness to the individual.
☒ Results in significant harm, embarrassment, inconvenient, or unfairness to the individual.

Please explain your response:

The HSPD-12 regulations and OMB guidance in Memorandum M-06-06 (February 17, 2006) require, at a minimum, that the FCC's Security Operations Center staff must conduct a background investigation and evaluation on all individuals who are granted access to the FCC's buildings, facilities, and information technology systems. Individuals who are granted higher level of access or are required to pass security clearance must undergo more extensive background investigations. Consequently, the personally identifiable information (PII) that this information system collects, maintains, and uses, and which is covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN is quite extensive, *e.g.*, includes a comprehensive collection of PII on the individual. Unauthorized disclosure or misuse of the PII could subject individuals to identity theft and other significant harm, embarrassment, inconvenience, or unfairness. Unauthorized disclosure could also endanger and/or compromised

the security of Federal employees and contractors in other Federal buildings and facilities as well as the buildings, facilities, and information technology services.

5.31 Is the impact level for the information system(s) covered by this system of records notice (SORN) consistent with the guidelines as determined by the FIPS 199 assessment?

☒ Yes
☐ No

Please explain your response:

Data in this information system, including paper files and electronic records, which is covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN, are required under HSPD-12 regulations and OMB guidance in Memorandum M-06-06 (February 17, 2006). The HSPD-12 regulations and OMB guidance are subject to the FIPS 199 assessment guidelines.

5.32 Has a "Certification and Accreditation" (C&A) been completed for the information system(s) covered this system of records notice (SORN)?

☒ Yes
☐ No

If yes, please explain your response and give the C&A completion date:

Data in this information system, including paper files and electronic records, which is covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN, are required under HSPD-12 regulations and OMB guidance in Memorandum M-06-06 (February 17, 2006). The C&A was completed in July 2008.

5.33 Has the Chief Information Officer (CIO) and/or the Chief Security Officer (CSO) designated this information system as requiring one or more of the following:

☒ Independent risk assessment: Required by HSPD-12 regulations and OMB Memorandum M-06-06 (February 17, 2006).
☒ Independent security test and evaluation: Required by HSPD-12 regulations and OMB Memorandum M-06-06 (February 17, 2006).
☐ Other risk assessment and/or security testing procedures, *etc.*:
☐ Not applicable:

5.34 Is the system using technology in ways that the Commission has not done so previously, *i.e.*, Smart Cards, Caller-ID, *etc*?

☒ Yes
☐ No

Please explain your response:

The HSPD-12 regulations and OMB Memorandum M-06-06 (February 17, 2006) require the FCC and other Federal agencies to implement PACS technology, *e.g.* ID badge system, *etc*., to assure that their buildings, facilities, and information technology systems are secure and accessible only to those individuals who have been granted the appropriate access level, based on the PII that the individuals have provided to the FCC and following the FCC's Security Operations Center's evaluation and analysis. This PII is covered under FCC/OMD-24, "Physical Access Control System (PACS)," SORN.

5.35 How does the use of the technology affect the privacy of the general public and FCC employees and contractors?

The FCC is required by OPM regulations and the HSPD-12 requirements to collect the background data and other personally identifiable information (PII) that is included in the paper files and electronic records in the information system covered by FCC/OMD-24, “Physical Access Control System (PACS),” SORN. The PACS was implemented to provide a secure and tamper-proof "universal" ID badge system for all individuals granted access to Federal buildings, facilities, and information technology systems. The degree of access is determined by each Federal agency. The FCC's Security Operations Center staff and others who collect, maintain, and use the PII data are instructed that the data are sensitive and that unauthorized use or disclosure of the data is prohibited under the Privacy Act of 1974, 5 U.S.C. 552a, *etc*.

5.36 Will the information system that is covered by this system of records notice (SORN) include a capability to identify, locate, and/or monitor individuals?

☒ Yes
☐ No

Please explain your response:

The information that is covered by FCC/OMD-24, “Physical Access Control System (PACS),” SORN is limited to the personally identifiable information (PII) on individuals as required by OPM regulations in Memorandum M-06-06 (February 17, 2006) and HSPD-12 requirements. The information is used to determine each individual's access to FCC and other Federal agency's buildings, facilities, and information technology systems. The requirements includes all current and former FCC and other Federal employees, contractors, consultants, temporary employees, visitors, students, interns, and all others who require access to FCC and other Federal buildings, facilities, and technology systems. The PACS includes a capability to identify, locate, and monitor all individuals location within these buildings and facilities, and their uses of information technology systems.

If the information system does not include any monitoring capabilities, please skip to **Section 6.0 Information Collection Requirements under the Paperwork Reduction Act (PRA):**

5.37 If the information system includes these technical capabilities identified in Questions 5.34 through 5.36 above, what kinds of information will be collected as a function of the monitoring of individuals?

The information system, covered by FCC/OMD-24, "Physical Access Control System (PACS)," SORN collects data about each individual's ingress, egress, and movements inside FCC buildings and facilities, and the use of information technology systems.

5.38 Does the information system covered by this system of records notice (SORN) contain any controls, policies, and procedures to prevent unauthorized monitoring?

☒ Yes
☐ No

Please explain your response:

The FCC's Security Operations Center staff has policy guidelines to insure that the data, which this information system compiles on each individual's ingress, egress, and movements inside FCC buildings and facilities, and the use of information technology systems, remain confidential and that the data are not to be disclosed except under specific circumstances, as determined by the

FCC's Office of the Managing Director's administrative policies governing the rights and responsibilities of FCC employees, contractors working at the FCC, frequent visitors, occasional visitors, students, interns, consultants, temporary hires, and all other individuals who are granted access to the FCC's buildings, facilities, and information technology systems, *etc*.

Section 6.0 Information Collection Requirements under the Paperwork Reduction Act (PRA):

6.1 Does this system of records notice (SORN) require non-FCC employees and contractors to perform any paperwork or recordkeeping activities?

☐ Yes, the public, *e.g.*, individuals, who are not FCC employees or contractions, are required to complete paperwork or recordkeeping functions or activities, *i.e.*, fill out forms and/or licensees, participate in surveys, and or maintain records *etc*.

Please explain your response:

☒ No, the public, *e.g.*, individuals, who are not FCC employees or contractors, are not required to perform any paperwork or recordkeeping functions or activities

Please explain your response:

The personally identifiable information (PII) contained in the paper files and electronic records that are included in this information system, which are covered by FCC/OMD-24, "Physical Access Control System (PACS)" SORN, also includes information about FCC employees and contractors working at the FCC. FCC employees are required to complete their Federal employment applications prior to hiring.

☐ No, this system of records notice includes only FCC employees and/or contractors, which exempts it from the PRA. Please skip to **Section 7.0 Correction and Redress:**

6.2 If the website requests information, such as the information necessary to complete an FCC form, license, authorization, *etc*., has the information collection covered by this system of records notice (SORN) been identified for possible inclusion under the FCC's Paperwork Reduction Act (PRA) requirements?

☒ Yes
☐ No

Please explain your response:

The employment applications and background applications fall under the PRA requirements. All applications, forms, *etc*., covered by this information system have been approved by OMB under the PRA.

FCC Form A-600, FCC Employee Identification Badge Form, and FCC Contractor Identification Badge Form are used only for FCC employees and contractors working at the FCC.

The FCC Frequent Visitor Badge Form is used for those individuals who are frequent, regular visitors to the FCC.

The FCC Visitor's Sign-in Sheet is used only for individuals who are visiting the FCC (one-time or infrequent visits).

These FCC forms do not require PRA approval.

If there are no PRA information collections associated with the information system or its applications, please skip to **Section 7.0 Correction and Redress:**

6.3 If yes, what PRA information collections covered by this system of records notice (SORN) are associated with this database please list the OMB Control Number, Title of the collection, Form number(s) as applicable, and Expiration date:

6.4 If there are any FCC forms associated with the information system(s) covered by this system of records notice (SORN), do the forms carry the Privacy Act notice?

☐ Yes

FCC Form Number(s) and Title(s):

☐ No
☐ Not applicable—the information collection does not include any forms.

6.5 Have the system managers contacted the Performance Evaluation and Records Management (PERM) staff to coordinate PRA requirements and submission of the information collection to the Office of Management and Budget?

☐ Yes
☐ No

Please explain your response:

Section 7.0 Correction and Redress:

7.1 Are the procedures for individuals wishing to inquire whether this system of records notice (SORN) contains information about them consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.554 – 0.555 for the Privacy Act and Freedom of Information Act (FOIA) requirements?

☒ Yes
☐ No

Please explain your response, and if this is an existing system of records notice (SORN), please specify what, if anything, is changing in this procedure:

Individuals wishing to inquire whether this system of records contains information about them should contact the FCC Security Operations Center (SOC) in the Administrative Operations Division of the Office of Managing Director (OMD-AO). Individuals must furnish their full name, birth date, Federal agency name, and work location for their records to be located and identified. An individual requesting notification of records in person must provide identity documents sufficient to satisfy the system manager of the records that the requester is entitled to access, *e.g.*, government-issued photo ID. Individuals requesting notification via mail or telephone must furnish, at a minimum, their name, date of birth, Social Security Number, and home address to establish identity. This is consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.554 – 0.555 for the Privacy Act and Freedom of Information Act (FOIA) requirements.

7.2 Are the procedures for individuals to gain access to their own records/information/data in this information system that is covered by this system of records notice (SORN) consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.554 – 0.555 for the Privacy Act and Freedom of Information Act (FOIA) requirements?

☒ Yes
☐ No

Please explain your response, and if this is an existing system of records notice (SORN), please specify what, if anything, is changing in this procedure:

Individuals wishing to request access to records about them should contact the Security Operations Center (SOC) in the Administrative Operations Division of the Office of Managing Director (OMD-AO). Individuals must furnish their full name (first, middle, and last name) and birth date for their record to be located and identified. An individual requesting access must also follow FCC Privacy Act regulations regarding verification of identify and access to records. This is consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.554 – 0.555 for the Privacy Act and Freedom of Information Act (FOIA) requirements.

7.3 Are the procedures for individuals seeking to correct or to amend records/information/data about them in the information system that is covered by this system of records notice (SORN) consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.556 – 0.558?

☒ Yes
☐ No

Please explain your response, and if this is an existing system of records notice (SORN), please specify what, if anything, is changing in this procedure:

Individuals wishing to request amendment of their records in FCC/OMD-24, "Physical Access Control System (PACS)" SORN should contact the Security Operations Center (SOC) in the Administrative Operations Division of the Office of Managing Director (OMD-AO). Individuals must furnish their full name (first, middle, and last name) and birth date for their record to be located and identified. An individual requesting amendment must also follow the FCC Privacy Act regulations regarding verification of identity and amendment of records. This is consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.556 – 0.558.

7.4 Does the FCC provide any redress to amend or correct information about an individual covered by this system of records notice (SORN), and if so, what alternatives are available to the individual, and are these consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.556 – 0.558?

☒ Yes
☐ No

Please explain your response:

Individuals seeking redress to amend or to correct information about themselves in FCC/OMD-24, "Physical Access Control System (PACS)" SORN should contact the Security Operations Center (SOC) in the Administrative Operations Division of the Office of Managing Director (OMD-AO). These individuals should also follow the FCC Privacy Act regulations regarding verification of identity and amendment of records. above. Individuals must furnish their full name (first, middle, and last name), birth date, for their record to be located and identified. This

is consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.556 – 0.558.

If this is a new system of records notice (SORN), please skip to Question 7.6.

7.5 Have the sources for the categories of records in the information system(s) covered by this system of records notice (SORN) changed?

☒ Yes
☐ No

Please explain your response, and if this is an existing system of records notice (SORN), please specify what, if anything, is changing in this procedure:

To comply with the requirements of HSPD-12 and the associated guidance provided in OMB Memorandum M-06-07 (February 17, 2006), the FCC has revised the sources of the categories of records in the information system, including the paper files and electronic records, which are covered by FCC/OMD-24, "Physical Access Control System (PACS)" SORN. The sources for the categories of records in the PACS information system include the individual FCC employee to whom the information applies, contractor, or applicant for employment; sponsoring agency; former sponsoring agency; other federal agencies; contract employer; and/or former employee..

7.6 Does this system of records notice (SORN) claim any exemptions to the notification, access, and correction, and/or amendment procedures as they apply to individuals seeking information about them in this SORN, and if so, are these exemptions consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.561?

☐ Yes
☒ No

Please explain your response, and if this is an existing system of records notice (SORN), please specify what, if anything, is changing in this procedure:

FCC/OMD-24, "Physical Access Control System (PACS)" SORN does not claim any exemptions to the notification, access, and correction, and/or amendment procedures as they apply to individuals seeking information about them in this SORN. This is consistent with the FCC Privacy Manual procedures and FCC rules under 47 CFR §§ 0.561 (3), (d), (e)(4)(G), (H), and (I), and (f) of the Privacy Act of 1974, 5 U.S.C. 552a, and from 47 CFR 0.554 – 0.557 of the Commission's rules.

7.7 What processes are in place to monitor and to respond to privacy and/or security incidents? Please specify what is changing if this is an existing system of records notice (SORN) that is being updated or revised?

The FCC's Security Operations Center (SOC) in the Administrative Division of the Office of Managing Director (OMD-AO) has posted notices that the information covered by FCC/OMD-24, “Physical Access Control System (PACS)” SORN, including the paper files and electronic databases, is information that is "non public for internal use only." The SOC also issues reminders periodically to those granted access to the information that they are to keep the information confidential and to safeguard all printed materials.

7.8 How often is the information system audited to ensure compliance with FCC and OMB regulations and to determine new needs?

- ☐ Six months or less
- ☐ One year
- ☐ Two years
- ☐ Three years
- ☐ Four years
- ☐ Five years
- ☒ Other audit scheduling procedure(s): Although this information system does not have an audit requirement, the FCC's Security Operations Center staff does have procedures, identified elsewhere in this PIA, noting the administrative protections, privacy training, and access controls that are in place to safeguard the personally identifiable information contained in this information system covered by FCC/OMD-24, "Physical Access Control System (PACS)" SORN.

Section 8.0 Consumer Satisfaction:

8.1 Is there a customer satisfaction survey included as part of the public access to the information covered by this system of records notice (SORN)?

- ☐ Yes
- ☐ No
- ☒ Not applicable

Please explain your response:

If there are no Consumer Satisfaction requirements, please skip to **Section 9.0 Risk Assessment and Mitigation:**

8.2 Have any potential Paperwork Reduction Act (PRA) issues been addressed prior to implementation of the customer satisfaction survey?

- ☐ Yes
- ☐ No

Please explain your response:

8.3 If there are PRA issues, were these issues addressed in the PRA component of this PIA template?

- ☐ Yes
- ☐ No

Please explain your response:

Section 9.0 Risk Assessment and Mitigation:

9.1 What are the potential privacy risks for the information covered by this system of records notice (SORN), and what practices and procedures have you adopted to minimize them?

Risks:	Mitigating factors:
a. Personally identifiable information (PII) in these paper files and in the electronic records may be inadvertently disclosed.	a. The FCC's Security Operations Center (SOC) staff who administers FCC/OMD-24, "Physical Access Control System (PACS)," SORN have numerous safeguards in place to minimize the inadvertent disclosure of this PII. The SOC staff is required to undergo a review of their credentials at least every five years.-
b. Some of the information system's personally identifiable information (PII) include paper documents that are stored in file cabinets.	b. PII that is contained in paper documents is stored in locked file cabinets, which are located in rooms that are locked when not in use.
c. Some of the information system's personally identifiable information (PII) includes electronic records that are stored in the FCC's computer network databases.	c. PII that is contained in electronic records is protected in the FCC's computer network databases, which require users to provide log-ins and access rights to these records.

9.2 What deficiencies did the bureau/office find in its procedures for evaluating the information system(s) covered by this system of records notice (SORN) and what remedies did the bureau/office enact following this Privacy Impact Assessment (PIA)?

Deficiencies:	Remedies:
a. Privacy notices are not posted in all conspicuous places where individuals must comply with the requirements of HSPD-12 and OMB guidance in Memorandum M-06-06.	a. The FCC's Security Operations Center will post privacy notices, as necessary.

9.3 What is the projected production/implementation date for the database(s):

Initial implementation:	April 2006
Secondary implementation:	September 2006
Tertiary implementation:	October 2008
Other implementation:	

9.4 Are there any ancillary and/or auxiliary information system(s) applications linked to this information system that is covered by this system of records notice (SORN), which may also require a Privacy Impact Assessment (PIA)?

☐ Yes
☒ No

If so, please state the application(s), if a Privacy Impact Assessment (PIA) has been done, and the completion date for PIA: