

## Background

EPA participates with other Federal agencies, state and tribes in the Mississippi River/Gulf of Mexico Watershed Nutrient Task Force. In 2001, the Task Force released the *Action Plan for Reducing, Mitigating and Controlling Hypoxia in the Northern Gulf of Mexico* (or *Action Plan* available at <http://www.epa.gov/msbasin/taskforce/actionplan.htm>). The *Action Plan* was informed by the science described in *An Integrated Assessment of Hypoxia in the Northern Gulf of Mexico* (or *Integrated Assessment* (available at [http://www.noaa.gov/products/hypox\\_finalfront.pdf](http://www.noaa.gov/products/hypox_finalfront.pdf)) developed by the National Science and Technology Council, Committee on Environment and Natural Resources. Six technical reports provided the scientific foundation for the *Integrated Assessment* and are available at [http://www.nos.noaa.gov/products/pub\\_hypox.html](http://www.nos.noaa.gov/products/pub_hypox.html). The aforementioned documents provide a comprehensive summary of the state-of-the-science for the Gulf of Mexico hypoxic zone to about the year 2000.

EPA's Office of Water has requested that the SAB develop a report that evaluates the state-of-the-science regarding the causes and extent of hypoxia in the Gulf of Mexico, as well as the scientific basis of possible management options in the Mississippi River Basin. The SAB is asked to focus on scientific advances since 2000 that may have increased scientific understanding and control options in three general areas.

1. *Characterization the Cause(s) of Hypoxia.* The physical, biological and chemical processes that affect the development, persistence and extent of hypoxia in the northern Gulf of Mexico.

2. *Characterization of Nutrient Fate, Transport and Sources.* Nutrient loadings, fate, transport and sources in the Mississippi River that impact Gulf hypoxia.

3. *Scientific Basis for Goals and Management Options.* The scientific basis for, and recommended revisions to, the goals proposed in the *Action Plan*; and the scientific basis for the efficacy of recommended management actions to reduce nutrient flux from point and nonpoint sources.

In response to EPA's request, the SAB Staff Office has formed the SAB Hypoxia Advisory Panel. Background on the Panel formation process was provided in a **Federal Register** notice published on February 17, 2006 (71 FR 8578–8580). Background for the first meeting of the SAB Hypoxia Advisory Panel was announced in a **Federal**

**Register** notice published on August 9, 2006 (71 FR 45543–45544). At its first meeting on September 6–7, 2006 the Panel organized itself into three subgroups corresponding to the three general areas described above. General information about the SAB Hypoxia Advisory Panel, as well as any updates concerning the teleconferences announced in this notice, may be found on the SAB Web site at: <http://www.epa.gov/sab>.

*Availability of Meeting Materials:* Pursuant to the Federal Advisory Committee Act, Public Law 92–463, notice is hereby given that the SAB Hypoxia Advisory Panel Subgroups will hold the seven public teleconferences on the dates and times provided above. Rosters of the SAB Hypoxia Advisory Panel, their biosketches, and the teleconference agendas will be posted on the SAB Web site <http://www.epa.gov/sab> prior to the teleconference.

*Procedures for Providing Public Input:* The SAB Staff Office accepts written public statements of any length, and accommodates oral public statements whenever possible. The SAB Staff Office expects that public statements presented at SAB meetings will not repeat previously submitted oral or written statements. *Oral Statements:* In general, individuals or groups requesting an oral presentation at a teleconference meeting will usually be limited to three minutes per speaker with no more than a total of fifteen minutes for all speakers. Interested parties should contact the appropriate DFO at the contact information provided above in writing via e-mail at least 10 days prior to the scheduled teleconference to be placed on the public speaker list for the teleconference. Speakers should provide an electronic copy of their statements to the DFO for distribution to interested parties and participants in the meeting. *Written Statements:* Written statements should be received in the SAB Staff Office at least seven days before scheduled teleconference so that the statements may be made available to the Panel for their consideration. Statements should be supplied to the appropriate DFO at the address and contact information provided above in the following formats: One hard copy with original signature, and one electronic copy via e-mail (acceptable file format: Adobe Acrobat, WordPerfect, Word, or Rich Text files in IBM-PC/Windows 98/2000/XP format).

*Meeting Accommodations:* Individuals requiring special accommodation to access the teleconference should contact the appropriate DFO at the phone number

or e-mail address noted above at least five business days prior to the meeting so that appropriate arrangements can be made.

Dated: September 15, 2006.

**Anthony F. Maciorowski,**  
Associate Director for Science, EPA Science  
Advisory Board Staff Office.

[FR Doc. 06–8177 Filed 9–22–06; 8:45 am]

BILLING CODE 6560–50–P

## FEDERAL COMMUNICATIONS COMMISSION

### Privacy Act System of Records

**AGENCY:** Federal Communications Commission (FCC or Commission).

**ACTION:** Notice; two altered Privacy Act systems of records; addition and/or modification of routine uses.

**SUMMARY:** Pursuant to subsection (e)(4) of the Privacy Act of 1974, as amended (5 U.S.C. 552a), the FCC proposes to change the name and alter two system of records, FCC/OMD–16, “Personal Security Files” (formerly “Personnel Investigation Records”) and FCC/OMD–24, “Physical Access Control System (PACS)” (formerly “Access Control System”). The two altered systems of records incorporate changes pursuant to the FCC's compliance with the Homeland Security Presidential Directive 12 (HSPD–12). The FCC will alter what information is maintained; the authority under which the systems of records are maintained; the purposes for which the information is maintained; add or modify the routine uses; revise the policies and practices for how the information is stored, safeguarded, retained, and disposed of; and will make other edits and revisions as necessary to comply with HSPD–12 implementation requirements and associated guidance provided in OMB Memorandum M–06–06 (February 17, 2006).

**DATES:** In accordance with subsections (e)(4) and (e)(11) of the Privacy Act of 1974, as amended (5 U.S.C. 552a), any interested person may submit written comments concerning the alteration of these two systems of records on or before October 25, 2006. Pursuant to Appendix I, 4(e) of OMB Circular A–130, the FCC is asking the Office of Management and Budget (OMB), which has oversight responsibility under the Privacy Act, to grant a waiver of the 40 day review period by OMB, the House of Representatives, and the Senate for this system of records. The FCC is requesting this waiver to comply with the deadline for implementation of the

HSPD-12 requirements. The two proposed altered systems shall be effective on October 25, 2006 unless the FCC receives comments that require a contrary determination. The Commission will publish a document in the **Federal Register** notifying the public if any changes are necessary. As required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, the FCC is submitting reports on these proposed altered systems to OMB and to both Houses of Congress.

**ADDRESSES:** Comments should be sent to Leslie F. Smith, Privacy Analyst, Performance Evaluation and Records Management (PERM), Room 1-C216, Federal Communications Commission (FCC), 445 12th Street, SW., Washington, DC 20554, (202) 418-0217, or via the Internet at [Leslie.Smith@fcc.gov](mailto:Leslie.Smith@fcc.gov). Comments may also be sent to Hillary A. Jaffe, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget, New Executive Office Building, 725 17th Street, NW., Washington, DC 20503, fax (202) 395-5167, or via the Internet at [Hillary\\_A.\\_Jaffe@omb.eop.gov](mailto:Hillary_A._Jaffe@omb.eop.gov).

**FOR FURTHER INFORMATION CONTACT:** Leslie F. Smith, Performance Evaluation and Records Management (PERM), Room 1-C216, Federal Communications Commission, 445 12th Street, SW., Washington, DC 20554, (202) 418-0217 or via the Internet at [Leslie.Smith@fcc.gov](mailto:Leslie.Smith@fcc.gov).

**SUPPLEMENTARY INFORMATION:** As required by the Privacy Act of 1974, as amended, 5 U.S.C. 552a(e)(4) and (e)(11), this document sets forth notice of the proposed alteration of two systems of records maintained by the FCC; and addition and/or modification of the routine uses. The FCC previously gave complete notice of the system of records covered under this Notice by publication in the **Federal Register** on April 5, 2006 (71 FR 17234) for FCC/ OMD-16, "Personal Security Files," and on October 23, 2000, (65 FR 63468) for FCC/ OMD-24, "Physical Access Control System (PACS)." This notice is a summary of the more detailed information about the two proposed altered systems of records, which may be viewed at the location given above in the **ADDRESSES** section. The purposes for altering FCC/ OMD-16, "Personnel Security Files" and FCC/ OMD-24, "Physical Access Control System (PACS)," are to change the name of each system of records; to change the information that is being maintained; to change the statutory authority under which information is maintained; to add or modify the routine uses; to change

the policies and practices for storage, retrieval, retention, access, and disposal of information; and otherwise to alter, update, and revise the two systems of records, as necessary, to comply with the requirements for implementation of HSPD-12 and to adhere to the guidance provided in OMB Memorandum M-06-06 (February 17, 2006).

The FCC proposes to achieve these purposes by altering each system of records with these changes: FCC/ OMD-16, "Personnel Security Files" (formerly "Personnel Investigation Records") with these changes:

Changes in the information that is being maintained; changes in the authority under which the information is collected and maintained; changes to the purposes for maintaining the information; and changes to the policies for storing, retrieving, accessing, retaining, adding and/or modifying the routine uses; disposing of records in the two systems of records to make them compliant with the requirements of HSPD-12. All these changes are done to adhere to the guidelines contained in OMB Memorandum M-06-06 (February 17, 2006).

The proposed routine uses for FCC/ OMD-16, Personnel Security Files, are:

1. Litigation by the Department of Justice—when (a) the FCC or any component thereof; or (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the Department of Justice (DOJ) has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation and the use of such records by the DOJ is therefore deemed by the FCC to be for a purpose compatible with the purpose for which the FCC collected the records.

2. A Court or Adjudicative Body—in a proceeding when: (a) The FCC or any component thereof; (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the Department of Justice (DOJ) has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the FCC to be for a purpose that is compatible with the purpose for which the FCC collected the records;

3. Law Enforcement and Investigation—except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of a law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, otherwise, responsible for enforcing, investigating, or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving entity.

4. Congressional Inquiries—when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;

5. Government-wide Program Management and Oversight—when requested by the National Archives and Records Administration or the General Services Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act, or when necessary to the review of private relief legislation pursuant to OMB Circular A-19;

6. Contract Services, Grants, or Cooperative Agreements—a record may be disclosed to FCC contractors, grantees, or volunteers who have been engaged to assist the FCC in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a.

7. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the agency—disclosure may be made to a Federal, State, or local government maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if

necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the FCC or to another Federal agency for criminal, civil, administrative personnel, or regulatory action;

8. **Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions** by other than the agency—disclosure may be made to a Federal, State, local, or tribal government or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the FCC or to another Federal agency for criminal, civil, administrative personnel, or regulatory action

9. **Labor Relations**—disclosure may be made to officials of labor organizations recognized under 5 U.S.C. Chapter 71 upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

10. **National Security and Intelligence Matters**—disclosure of these records may be disclosed to Federal, State, local agencies, or other appropriate entities or individuals, or through established liaison channels to selected foreign government in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947, as amended, the CIA Act of 1949, as amended, Executive Order 12333 or any successor order, applicable to national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders, or directives.

The FCC will use the records in FCC/ OMD-16, "Personal Security Files," to conduct background investigations to determine compliance with Federal regulations and/or to make a determination about an individual's suitability, eligibility, and fitness for Federal employment or contractual services, access to classified materials and/or restricted areas, to evaluate the appropriate security clearance(s), and to take action on or to respond to a complaint about a threat, harassment, intimidation, violence, or other inappropriate behavior involving FCC employees, interns, volunteers, and contractors.

The proposed routine uses for FCC/ OMD-24, Physical Access Control System (PACS), are:

1. **Litigation by the Department of Justice**—when (a) the FCC or any component thereof; or (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the FCC or the Department of Justice (DOJ) has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation and the use of such records by the DOJ is therefore deemed by the FCC to be for a purpose compatible with the purpose for which the FCC collected the records.

2. **Court or Adjudicative Body**—in a proceeding when: (a) The FCC or any component thereof; (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the Department of Justice (DOJ) has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the FCC to be for a purpose that is compatible with the purpose for which the FCC collected the records;

3. **Law Enforcement and Investigation**—except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of a law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign,

State, local, or tribal, otherwise, responsible for enforcing, investigating, or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving entity.

4. **Congressional Inquiries**—when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;

5. **Government-wide Program Management and Oversight**—when requested by the National Archives and Records Administration or the General Services Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act, or when necessary for the review of private relief legislation pursuant to OMB Circular No. A-19;

6. **Contract Services, Grants, or Cooperative Agreements**—a record may be disclosed to FCC contractors, grantees, or volunteers who have been engaged to assist the FCC in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a.

7. **Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions** by the agency—disclosure may be made to a Federal, State, or local government maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit;

8. **Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions** by other than the agency—disclosure may be made to a Federal, State, local, or tribal government, or other public authority of

the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire records if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel or regulatory action;

9. Labor Relations—A record from this system may be disclosed to officials of labor organizations recognized under 5 U.S.C. Chapter 71 upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

10. National Security and Intelligence Matters—disclosure of these records may be disclosed to Federal, State, local agencies, or other appropriate entities or individuals, or through established liaison channels to selected foreign government in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947, as amended, the CIA Act of 1949, as amended, Executive Order 12333 or any successor order, applicable to national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders, or directives;

11. Invalid PIV Card Notification—disclosure may be made to notify another Federal agency, when, or to verify whether, a PIV card is no longer valid; and

**Note:** 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.* The FCC will use records in FCC/OMD-24, "Physical Access Control System (PACS)," to ensure the safety and security of FCC facilities, systems, and information, employees, contractors, interns, guests, frequent visitors, while they are within the FCC buildings and facilities; to

verify that all individuals entering the FCC buildings and other Federal facilities, and using FCC and Federal information resources have such authorization; and to track and control FCC badges issued to individuals entering and existing FCC facilities, using FCC systems, and/or accessing classified information.

This notice meets the requirement documenting the change in the two FCC systems of records, and provides the public, Congress, and the Office of Management and Budget (OMB) an opportunity to comment.

#### FCC/OMD-16

##### SYSTEM NAME:

Personnel Security Files.<sup>1</sup>

##### SECURITY CLASSIFICATION:

Most personnel identity verification records are not classified. However, in some cases, records of certain individuals, or portions of some records may have national defense/foreign policy classifications.

##### SYSTEM LOCATION:

Security Operations Center, Office of Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-B458, Washington, DC 20554.

##### CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Information includes:

1. Current and former Federal Communications Commission (FCC) employees, including Commission retirees and those who resigned from the Commission, other Federal employees, applicants for employment in the Federal service or contracts, contractors of the FCC, experts, instructors, consultants to FCC and other Federal programs, visitors, and all others who may require regular, on-going access to FCC and other Federal facilities, information technology systems, or information classified in the interest of national security, and individuals formerly in any of these positions;

2. Individuals who are authorized to perform or to use services provide in FCC facilities, *e.g.*, FCC credit union and employee assistance program staff (EAP); and

3. Individuals who are neither applicants nor employees of the Federal Government, but who are or were involved in Federal programs under a co-operative agreement, *e.g.*, students and interns.

##### CATEGORIES OF RECORDS IN THE SYSTEM:

Information includes:

1. Data needed to identify an individual, including: Individual's last, first, middle names (filed alphabetically by last name), and former name(s) (as applicable); Social Security Number; date of birth; birthplace; home address; home telephone number(s); residential history; organizational unit; position title;

2. Individual's citizenship; security classification; types and dates of investigations; and agency conducting investigation, investigation dates, security clearance(s) and grant date(s), and position sensitivity level(s); and miscellaneous investigation comments;

3. Names of relatives; birth date(s), home address, and citizenship; relatives who work for the Federal government;

4. Reports about the individual's qualifications for a position, *e.g.*, employee/applicant's employment/work history, summary report of investigation, results of suitability decisions, employment references and contact information; and educational/training institutions attended, degrees and certifications earned, and educational and training references;

5. Information needed to investigate an individual's character, conduct, and behavior in the community where he or she lives or lived; criminal history, *e.g.*, arrests and convictions for violations against the law; mental health history; drug use; financial information, *e.g.*, income tax return information and credit reports; reports of interviews with present and former supervisors, co-workers, associates, educators, and other related personal references and contact information;

6. Reports of inquiries with law enforcement agencies, employers, and reports of action after the Office of Personnel Management or FBI Section 8(d) Full Field Investigation; Notices of Security Investigation and other information developed from the above described Certificates of Clearance, *e.g.*, date of security clearances, requests for appeals, witness statements, investigator's notes, security violations, circumstances of violations, and agency action(s) taken;

7. Information needed to investigate allegations of FCC employee's misconduct;

8. Information needed to investigate miscellaneous complaints not covered by the FCC's formal or informal grievance procedure;

9. Information needed to conduct inquiries under the "President's Program to Eliminate Waste and Fraud in Government;" and

10. Information needed to investigate violence, threats, harassment, intimidation, or other inappropriate

<sup>1</sup> This system of records was formerly titled "Personnel Investigation Records."

behavior causing an FCC employee, contractor, or visitor(s) to fear for his/her personal safety in the FCC workplace: Case number, victim's name, office telephone number, room number, organizational unit, duty station, position, supervisor, supervisor's telephone number, location of incident, activity at time of incident, circumstances surrounding the incident, perpetrator, name(s) and telephone number(s) of witness(es), injured party(s), medical treatment(s), medical report, property damages, report(s) to police and/or Federal Protective Services, and related miscellaneous information.

11. Information obtained from SF-85, SF-85P, SF-86, and SF-87 forms; summary reports from OPM or another Federal agency conducting background investigations; and results of adjudications and security violations. (**NOTE:** This system of records does not duplicate or supersede the Office of Personnel Management (OPM) Central-9 system of records, which covers the investigations OPM and its contractors conduct on behalf of other agencies.)

#### **AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

Depending upon the purpose(s) for the investigation, the U.S. government is authorized to ask for this information under 5 U.S.C. 1303, 1304, 3301, 7902, 9101; 42 U.S.C. 2165 and 2201; 50 U.S.C. 781 to 887; 5 CFR Parts 5, 732, and 736; Executive Orders 9397, 10450, 10865, 12196, 12333, 12356, and 12674; and Homeland Security Presidential Directive (HSPD) 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004.

#### **PURPOSE(S):**

FCC Security Officer and the Personnel Security Specialist use this information to document and support decisions:

1. To determine compliance with Federal regulations and/or to make a determination about an individual's suitability, eligibility, and fitness for Federal employment, access to classified information or restricted areas, position sensitivity, security clearances, evaluations of qualifications, and loyalty to the United States, and to document such determinations;

2. To evaluate an applicant's qualifications and suitability to perform contractual services for the U.S. Government and to document such determinations;

3. To evaluate the eligibility and suitability of students, interns, or volunteers to the extent that their duties require access to FCC and other Federal

facilities, information, systems, or applications, and to document such determinations;

4. To respond to a written inquiry conducted under the "President's Program to Eliminate Waste and Fraud in the Government;"

5. To take action on, or to respond to a complaint about a threat, harassment, intimidation, violence, or other inappropriate behavior involving one or more FCC employees and/or contract employees, and to counsel employees; and

6. To document security violations and supervisory actions taken.

#### **ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Litigation by the Department of Justice—when (a) the FCC or any component thereof; or (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the Department of Justice (DOJ) has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation and the use of such records by the DOJ is therefore deemed by the FCC to be for a purpose compatible with the purpose for which the FCC collected the records.

2. A Court or Adjudicative Body—in a proceeding when: (a) The FCC or any component thereof; (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the Department of Justice (DOJ) has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the FCC to be for a purpose that is compatible with the purpose for which the FCC collected the records;

3. Law Enforcement and Investigation—except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of a law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by

regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, otherwise, responsible for enforcing, investigating, or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving entity.

4. Congressional Inquiries—when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;

5. Government-wide Program Management and Oversight—when requested by the National Archives and Records Administration or the General Services Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act, or when necessary to the review of private relief legislation pursuant to OMB Circular A-19;

6. Contract Services, Grants, or Cooperative Agreements—a record may be disclosed to FCC contractors, grantees, or volunteers who have been engaged to assist the FCC in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a.

7. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the agency—disclosure may be made to a Federal, State, or local government maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit. The other agency or licensing organization may then make a request supported by

the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the FCC or to another Federal agency for criminal, civil, administrative personnel, or regulatory action;

8. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by other than the agency—disclosure may be made to a Federal, State, local, or tribal government, or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the FCC or to another Federal agency for criminal, civil, administrative personnel, or regulatory action.

9. Labor Relations—disclosure may be made to officials of labor organizations recognized under 5 U.S.C. Chapter 71 upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

10. National Security and Intelligence Matters—disclosure of these records may be disclosed to Federal, State, local agencies, or other appropriate entities or individuals, or through established liaison channels to selected foreign government in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947, as amended, the CIA Act of 1949, as amended, Executive Order 12333 or any successor order, applicable to national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders, or directives.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

#### **DISCLOSURE TO CONSUMER REPORTING AGENCIES:**

None.

#### **POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

##### **STORAGE:**

Information is stored on paper records, which are stored in file folders in security containers, and in electronic records that are maintained in a stand-alone computer database.

##### **RETRIEVABILITY:**

Records are retrieved by an individual's name or Social Security Number (SSN).

##### **SAFEGUARDS:**

Comprehensive paper records are maintained in file folders and stored in approved security containers, which are locked and located within a secure, access-controlled area. Access is limited to approved security office and administrative personnel who have a need for them in the performance of their official duties, *e.g.*, who have responsibility for suitability determinations. Paper records limited (in number and scope) are kept in the FCC's regional offices and laboratory facilities in locked metal file cabinets in locked rooms.

Comprehensive electronic records are maintained in networked computer database(s). The computer database is secured through controlled access and passwords restricted to Federal employee and contractor security and administrative personnel on a "need to know" basis, *e.g.*, who have a need for them in the performance of their official duties, *e.g.*, who have responsibility for suitability determinations. Access to the records is restricted to those with a specific role in the Personal Identification Verification (PIV) process that requires access to background investigation forms to perform their duties, and who have been given a password to access that part of the system including background investigation records. The FCC Security Office staff maintains an audit trail. Individuals given roles in the PIV process must complete training specific to their roles to ensure that they are knowledgeable about how to protect individually identifiable information. The databases are backed-up on a daily basis to floppy disk(s), which are then stored in a secured area.

##### **RETENTION AND DISPOSAL:**

These records are retained and disposed of in accordance with General Records Schedule 18, item 22a, approved by the National Archives and Records Administration (NARA). Both paper and electronic records are retained during employment or while an

individual is actively involved in Federal programs. As appropriate, records are returned to investigating agencies after employment terminates; otherwise, the records are destroyed upon notification of death or not later than five years after the employee's retirement or separation from the FCC, or the employee's transfer to another Federal agency or department, whichever is applicable.

In accordance with NARA guidelines, the FCC destroys paper records by shredding; and electronic records are destroyed by electronic erasure. Individuals interested in further information about retention and disposal may request a copy of the disposition instructions from the FCC Privacy Act Officer.

##### **SYSTEM MANAGER(S) AND ADDRESS:**

Security Operations Center, Office of the Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-B458, Washington, DC 20554.

##### **NOTIFICATION PROCEDURE:**

Under the authority granted to heads of agencies by 5 U.S.C. 552a (k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its notification procedure for this system of records.

##### **RECORD ACCESS PROCEDURES:**

Under the authority granted to heads of agencies by 5 U.S.C. 552a (k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its record access procedures for this system of records.

##### **CONTESTING RECORD PROCEDURE:**

Under the authority granted to heads of agencies by 5 U.S.C. 552a (k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its contesting record procedure for this system of records.

##### **RECORD SOURCE CATEGORIES:**

Under the authority granted to heads of agencies by 5 U.S.C. 552a (k), the FCC has determined (47 CFR 0.561) that this system of records is exempt from disclosing its record sources for this system of records.

##### **EXEMPTION FROM CERTAIN PROVISIONS OF THE ACT:**

This system of records is exempt from sections (c)(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. These provisions concern the notification, record access, and contesting procedures described above, and also

the publication of record sources. The system is exempt from these provisions because it contains the following types of information:

1. Investigative material compiled for law enforcement purposes as defined in Section (k)(2) of the Privacy Act;

2. Properly classified information, obtained from another Federal agency during the course of a personnel investigation, which pertains to national defense and foreign policy, as stated in Section (k)(1) of the Privacy Act; and

3. Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, as described in Section (k)(5) of the Privacy Act, as amended. (Information will be withheld to the extent it identifies witnesses promised confidentiality as a condition of providing information during the course of the background investigation.)

#### **FCC/OMD-24**

##### **SYSTEM NAME:**

Physical Access Control System (PACS)<sup>2</sup>

##### **SECURITY CLASSIFICATION:**

None.

##### **SYSTEM LOCATION:**

Information in this system is maintained in the following location: Security Operations Center, Office of the Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-B458, Washington, DC 20554. This location is in a Federal building, where staffed guard stations have been established and which has an installed Personal Identity Verification (PIV) card reader system.

##### **CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

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 employees.

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.

##### **CATEGORIES OF RECORDS IN THE SYSTEM:**

The system consists of a computer database containing records on those individuals to whom the FCC has issued credentials. The records are filed alphabetically by last name, with a corresponding badge number.

1. FCC employee/temporary hire database includes: Full name (first, middle, and last names), Social Security Number (SSN), birth date, signature, image (photograph), fingerprints, hair color, eye color, height, weight, FCC telephone number, FCC Bureau/Office, FCC office/room number, personal identification number (PIN), background investigation form data and results, date the personal identify verification (PIV) card was issued and expiration dates, PIV registrar approval signature, PIV card serial number, emergency responder designation, copies of documents verifying identification or information derived from such documents, *e.g.* document title, document issuing authority, document number, document expiration date, other document information), national security level clearance and expiration date, parking permit data, computer system user name, user access and permission rights, authentication certificates, and digital signature information.

2. Contractor database includes: First, middle, and last name, Social Security Number (SSN), birth date, signature, image (photograph), fingerprints, hair color, eye color, height, weight, contractor company name, Federal supervisor, telephone number, FCC point of contact, FCC Bureau/Office, FCC office/room number, FCC telephone number, and FCC contractor badge number, personal identification number (PIN), background investigation form data and results, date the personal identify verification (PIV) card was

issued and expiration dates, PIV registrar approval signature, PIV card serial number, emergency responder designation, copies of documents verifying identification or information derived from such documents, *e.g.*, document title, document issuing authority, document number, document expiration date, other document information), national security level clearance and expiration date, parking permit data, computer system user name, user access and permission rights, authentication certificates, and digital signature information.

3. Frequent Visitor's database includes: First and last names, employer's name, address, telephone number, image (photograph), and date of issuance and expiration date.

4. Day contractor database includes: First and last name along with badge number, date of issuance and expiration date.

5. Visitor database includes: First and last name, image (photograph), FCC point of contact and date of issuance.

6. Special Parking Access database includes: First and last name, telephone number, employer, FCC point of contact, and date of issuance.

**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.

##### **AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

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.

##### **PURPOSE(S):**

The purposes of the system are:

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

<sup>2</sup> This system of records was formerly titled "Access Control System."

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.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

1. Litigation by the Department of Justice—when (a) the FCC or any component thereof; or (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the FCC or the Department of Justice (DOJ) has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation and the use of such records by the DOJ is therefore deemed by the FCC to be for a purpose compatible with the purpose for which the FCC collected the records;

2. Court or Adjudicative Body—in a proceeding when: (a) The FCC or any component thereof; (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the Department of Justice (DOJ) has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the FCC to be for a purpose that is compatible with the purpose for which the FCC collected the records;

3. Law Enforcement and Investigation—except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of a law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, otherwise, responsible for enforcing, investigating, or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order

issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving entity;

4. Congressional Inquiries—when requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for their own records;

5. Government-wide Program Management and Oversight—when requested by the National Archives and Records Administration or the General Services Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906; when the U.S. Department of Justice is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act; or when the Office of Management and Budget is contacted in order to obtain that office's advice regarding obligations under the Privacy Act, or when necessary for the review of private relief legislation pursuant to OMB Circular No. A-19;

6. Contract Services, Grants, or Cooperative Agreements—a record may be disclosed to FCC contractors, grantees, or volunteers who have been engaged to assist the FCC in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a;

7. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the agency—disclosure may be made to a Federal, State, or local government maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit;

8. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by other than the agency—disclosure may be made to a Federal, State, local, or tribal government, or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of

a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire records if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel or regulatory action;

9. Labor Relations—A record from this system may be disclosed to officials of labor organizations recognized under 5 U.S.C. Chapter 71 upon receipt of a formal request and in accord with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions;

10. National Security and Intelligence Matters—disclosure of these records may be disclosed to Federal, State, local agencies, or other appropriate entities or individuals, or through established liaison channels to selected foreign government in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947, as amended, the CIA Act of 1949, as amended, Executive Order 12333 or any successor order, applicable to national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders, or directives; and

11. Invalid PIV Card Notification—disclosure may be made to notify another Federal agency, when, or to verify whether, a PIV card is no longer valid.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

**Note:** 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.*

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

**STORAGE:**

The information is maintained in a password-protected or logical access

controlled electronic media, *e.g.*, computer database(s), and in securely controlled paper files.

#### RETRIEVABILITY:

The information can be retrieved by: (1) The name of the individual; (2) Social Security Number (SSN); (3) other ID number, *e.g.*, FCC employee, contractor, or frequent visitor badge number; or (4) PIV card serial number.

#### SAFEGUARDS:

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 role requires 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 FCC Security Operations Center staff 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.

#### RETENTION AND DISPOSAL:

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.

#### SYSTEM MANAGER(S) AND ADDRESS:

Security Operations Center, Office of Managing Director, Federal Communications Commission (FCC), 445 12th Street, SW., Room 1-B458, Washington, DC 20554.

#### NOTIFICATION PROCEDURE:

Individuals wishing to inquire whether this system of records contains information about them should contact the system manager indicated above. 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. *See* 47 CFR 0.554-0.555.

#### RECORD ACCESS PROCEDURES:

Individuals wishing to request access to records about them should contact the system manager indicated above. Individuals must furnish their full name (first, middle, and last name), birth date, for their record to be located and identified. An individual requesting access must also follow FCC Privacy Act regulations regarding verification of identity and access to records. *See* 47 CFR 0.554-0.555.

#### CONTESTING RECORD PROCEDURES:

Individuals wishing to request amendment of their records should contact the system manager indicated above. Individuals must furnish their

full name (first, middle, and last name), 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. *See* 47 CFR 0.556-0.557.

#### RECORD SOURCE CATEGORIES:

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.

#### EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Federal Communications Commission.

**Marlene H. Dortch,**

*Secretary.*

[FR Doc. 06-8182 Filed 9-22-06; 8:45 am]

**BILLING CODE 6712-01-P**

## FEDERAL RESERVE SYSTEM

### Change in Bank Control Notices; Acquisition of Shares of Bank or Bank Holding Companies

The notificants listed below have applied under the Change in Bank Control Act (12 U.S.C. 1817(j)) and § 225.41 of the Board's Regulation Y (12 CFR 225.41) to acquire a bank or bank holding company. The factors that are considered in acting on the notices are set forth in paragraph 7 of the Act (12 U.S.C. 1817(j)(7)).

The notices are available for immediate inspection at the Federal Reserve Bank indicated. The notices also will be available for inspection at the office of the Board of Governors. Interested persons may express their views in writing to the Reserve Bank indicated for that notice or to the offices of the Board of Governors. Comments must be received not later than October 10, 2006.

**A. Federal Reserve Bank of Philadelphia** (Michael E. Collins, Senior Vice President) 100 North 6th Street, Philadelphia, Pennsylvania 19105-1521:

1. *Paul C. Woelkers*, Moscow, Pennsylvania; to acquire voting shares of Landmark Community Bank, Pittston, Pennsylvania.

Board of Governors of the Federal Reserve System, September 20, 2006.

**Robert deV. Frierson,**

*Deputy Secretary of the Board.*

[FR Doc. E6-15661 Filed 9-22-06; 8:45 am]

**BILLING CODE 6210-01-S**