Form Number: N/A.

Type of Review: Revision of a currently approved collection.

Respondents: Business or other for-profit entities; Individuals or households; Not-for-profit institutions.

Number of Respondents and Responses: 50,151 respondents; 147,453,559 responses.

Estimated Time per Response: .004 hours (15 seconds) to 1 hour.

Frequency of Response: Recordkeeping requirement; Annual, on occasion and one-time reporting requirements; Third party disclosure requirement.

Obligation to Respond: Required to obtain or retain benefits. The statutory authority for the information collection requirements is found in the Telephone Consumer Protection Act of 1991 (TCPA), Public Law 102–243, December 20, 1991, 105 Stat. 2394, which added Section 227 of the Communications Act of 1934, [47 U.S.C. 227] Restrictions on the Use of Telephone Equipment.

Total Annual Burden: 712,140 hours.

Total Annual Cost: $3,989,700.

Nature and Extent of Confidentiality: Confidentiality is an issue to the extent that individuals and households provide personally identifiable information, which is covered under the FCC's system of records notice (SORN), FCC/CGB–1, ''Informal Complaints and Inquiries.'' As required by the Privacy Act, 5 U.S.C. 552a, the Commission also published a SORN, FCC/CGB–1 ''Informal Complaints and Inquiries'', in the **Federal Register** on December 15, 2009 (74 FR 66356) which became effective on January 25, 2010. A system of records for the do-not-call registry was created by the Federal Trade Commission (FTC) under the Privacy Act. The FTC originally published a notice in the **Federal Register** describing the system. *See* 68 FR 37494, June 24, 2003. The FTC updated its system of records for the do-not-call registry in 2009. *See* 74 FR 17863, April 17, 2009.

Privacy Impact Assessment: Yes. The Privacy Impact Assessment (PIA) was completed on June 28, 2007. It may be reviewed at: *http://www.fcc.gov/omd/privacyact/Privacy_Impact_Assessment.html.* The Commission is in the process of updating the PIA to incorporate various revisions made to the SORN.

Needs and Uses: The reporting requirements included under this OMB Control Number 3060–0519 enable the Commission to gather information regarding violations of Section 227 of the Communications Act, the Do-Not-Call Implementation Act (Do-Not-Call Act), and the Commission's implementing rules. If the information collection was not conducted, the Commission would be unable to track and enforce violations of Section 227 of the Communications Act, the Do-Not-Call Act, or the Commission's implementing rules. The Commission's implementing rules provide consumers with several options for avoiding most unwanted telephone solicitations.

The national do-not-call registry supplements the company-specific do-not-call rules for those consumers who wish to continue requesting that particular companies not call them. Any company that is asked by a consumer, including an existing customer, not to call again must honor that request for five (5) years.

A provision of the Commission's rules, however, allows consumers to give specific companies permission to call them through an express written agreement. Nonprofit organizations, companies with whom consumers have an established business relationship, and calls to persons with whom the telemarketer has a personal relationship are exempt from the ''do-not-call'' registry requirements.

On September 21, 2004, the Commission released the *Safe Harbor Order* establishing a limited safe harbor in which persons will not be liable for placing autodialed and prerecorded message calls to numbers ported from a wireline service within the previous 15 days. The Commission also amended its existing National Do-Not-Call Registry safe harbor to require telemarketers to scrub their lists against the Registry every 31 days.

On December 4, 2007, the Commission released the *DNC NPRM* seeking comment on its tentative conclusion that registrations with the Registry should be honored indefinitely, unless a number is disconnected or reassigned or the consumer cancels his registration.

On June 17, 2008, in accordance with the Do-Not-Call Improvement Act of 2007, the Commission revised its rules to minimize the inconvenience to consumers of having to re-register their preferences not to receive telemarketing calls and to further the underlying goal of the National Do-Not-Call Registry to protect consumer privacy rights. The Commission released a *Report and Order* in CG Docket No. 02–278, FCC 08–147, amending the Commission's rules under the Telephone Consumer Protection Act (TCPA) to require sellers and/or telemarketers to honor registrations with the National Do-Not-Call Registry so that registrations will not automatically expire based on the current five year registration period. Specifically, the Commission modified § 64.1200(c)(2) of its rules to require sellers and/or telemarketers to honor numbers registered on the Registry indefinitely or until the number is removed by the database administrator or the registration is cancelled by the consumer.

Most recently, on February 15, 2012, the Commission released a *Report and Order* in CG Docket No. 02–278, FCC 12–21, revising its rules to: (1) Require prior express written consent for all autodialed or prerecorded telemarketing calls to wireless numbers and for all prerecorded telemarketing calls to residential lines; (2) eliminate the established business relationship exception to the consent requirement for prerecorded telemarketing calls to residential lines; (3) require telemarketers to include an automated, interactive opt-out mechanism in all prerecorded telemarketing calls, to allow consumers more easily to opt out of future robocalls during a robocall itself; and (4) require telemarketers to comply with the 3% limit on abandoned calls during each calling campaign, in order to discourage intrusive calling campaigns.

Finally, the Commission also exempted from the Telephone Consumer Protection Act requirements prerecorded calls to residential lines made by health care-related entities governed by the Health Insurance Portability and Accountability Act of 1996.

Federal Communications Commission.

Marlene H. Dortch,

Secretary, Office of the Secretary, Office of Managing Director.

[FR Doc. 2012–12965 Filed 5–29–12; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL COMMUNICATIONS COMMISSION

Privacy Act System of Records

AGENCY: Federal Communications Commission.

ACTION: Notice; one new Privacy Act system of records.

SUMMARY: Pursuant to subsection (e)(4) of the *Privacy Act of 1974,* as amended (5 U.S.C. 552a), the Federal Communications Commission (FCC or Commission) proposes to add a new system of records, FCC/OMD–30, ''FCC Visitors Database.'' The FCC's Security Operations Center (SOC) in the Office of Managing Director (OMD) will use the information contained in FCC/OMD–30 to cover the personally identifiable information (PII) that all visitors to the

FCC, including but not limited to U.S. citizens, permanent residents (*i.e.,* green card holders), and foreign nationals, must provide to the SOC to gain admittance to the FCC headquarters buildings and other FCC facilities.

DATES: In accordance with subsections (e)(4) and (e)(11) of the Privacy Act, as amended, any interested person may submit written comments concerning this new system of records on or before June 29, 2012. The Office of Information and Regulatory Affairs (OIRA), Office of Management and Budget (OMB), which has oversight responsibility under the Privacy Act to review the system of records, and Congress may submit comments on or before July 9, 2012. The proposed new system of records will become effective on July 9, 2012 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, the FCC is submitting reports on this proposed new system to OMB and Congress.

ADDRESSES: Address comments 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, or via the Internet at *Leslie.Smith@fcc.gov.*

FOR FURTHER INFORMATION CONTACT: Contact Leslie F. Smith, 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.*

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 new system of records to be maintained by the FCC. This notice is a summary of the more detailed information about the proposed new system of records, which may be obtained or viewed pursuant to the contact and location information given above in the **ADDRESSES** section. The purpose for establishing this new system of records, FCC/OMD–30, ''FCC Visitors Database,'' is for the FCC's Security Operations Center (SOC) in the Office of Managing Director (OMD) to use this information to cover the personally identifiable information (PII) that all visitors to the FCC, including but not limited to U.S. citizens, permanent residents (*i.e.,* green card holders), and foreign nationals, must provide to the SOC to gain admittance to the FCC headquarters buildings and other FCC facilities.

This notice meets the requirement documenting the proposed new system of records that is to be added to the systems of records that the FCC maintains, and provides the public, OMB, and Congress with an opportunity to comment.

FCC/OMD–30

SYSTEM NAME:

FCC Visitors Database.

SECURITY CLASSIFICATION:

The FCC's Security Operations Center (SOC) has not assigned a security classification to this system of records.

SYSTEM LOCATION:

Office of the Managing Director (OMD), Security Operations Center (SOC), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554;

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The records in this system include all visitors to the FCC. These individuals include, but are not limited to U.S. citizens, permanent residents (*i.e.,* green card holders), and foreign nationals.

CATEGORIES OF RECORDS IN THE SYSTEM:

The categories of records in the FCC Visitors Database include, but are not limited to the individual's first and last name, photographic identification (including but not limited to a driver's license, passport, or other types of photo identification), the authority issuing the photo identification, U.S. visa number, FCC point of contact, visitor signature, professional title, organizational affiliation, contact information for the visitor, including but not limited to wireline and wireless (cell) phone numbers, correspondence related to information required to obtain visitor entry to the FCC, and purpose(s) for visiting the FCC.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 6 U.S.C. 202; 8 U.S.C. 1103, 1158, 1201, 1324, 1357, 1360, 1365a, 1365b, 1372, 1379, 1732; Federal Information Security Act (Pub. L. 104–106, sec. 5113); Electronic Government Act (Pub. L. 104–347, sec. 203); and Federal Property and Administrative Act of 1949, as amended.

PURPOSE(S):

The purpose of the system is to cover the personally identifiable information (PII) that all visitors to the FCC, including but not limited to U.S. citizens, permanent residents (*i.e.,* green card holders), and foreign nationals, must provide to the FCC's Security Operations Center (SOC) to gain admittance to the FCC headquarters buildings and other FCC facilities.

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; (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, State, local, tribal, or foreign, or otherwise responsible for enforcing, investigating, or prosecuting such violation or charged with enforcing or implementing the statute, 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. Government-wide Program Management and Oversight—When requested by the National Archives and Records Administration (NARA), the Government Accountability Office (GAO), and/or the General Services Administration (GSA) for the purpose of records management inspections conducted under authority of 44 U.S.C. §§ 2904 and 2906 (such disclosure(s)) shall not be used to make a determination about individuals); when the U.S. Department of Justice (DOJ) is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act (FOIA); or when the Office of Management and Budget (OMB) is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;

5. Congressional Inquiries—When requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for the individual's own records;

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, local, or tribal government, or other public authority or entity maintaining civil, criminal, intelligence, national security, 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 or entity 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 agency or to another Federal agency for criminal, civil, administrative, personnel or regulatory action;

9. National Security and Intelligence Matters—Disclosure of these records may be made to Federal, State, local agencies, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments and international law enforcement organizations and agencies in order to enable a Federal agency or entity charged with, but not limited to national security and/or intelligence activities and related functions, to carry out these duties and 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;

10. Department of State, Department of Homeland Security, and other Federal Agencies—A record from this system may be disclosed, where appropriate, to the State Department, Department of Homeland Security (DHS), and/or other Federal agencies and entities charged with, but not limited to national security, law enforcement, immigration, intelligence, and related functions, activities, duties, and responsibilities, where there is an indication of 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 enforce, investigate, or prosecute violations, or to enforce or implement a statute, rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving Federal agency or entity;

11. Foreign Governments—A record from this system may be disclosed through the U.S. Department of State or the Department of Homeland Security (DHS) or other Federal security agencies, entities, or organizations or directly to the representative of such a foreign government or country, to the extent necessary to assist such a government or country in apprehending and/or returning a fugitive to a jurisdiction which seeks the individual's return, or to assist such a country in civil or criminal proceedings in which the United States or one of its officers or agencies has an interest; and

12. Breach Notification—A record from this system may be disclosed to appropriate agencies, entities, and persons when: (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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.

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

STORAGE:

The information in the FCC Visitors Database includes paper document, files, and records that are stored in file cabinets in the Security Operations Center (SOC), and electronic records, files, and electronic records, files, and data that are stored in the FCC's computer network databases.

RETRIEVABILITY:

The information in the FCC Visitors Database may be retrieved by the name of the individual, driver's license number, U.S. passport number, foreign passport number, U.S. visa number, date of birth (DOB), and/or photo ID number.

SAFEGUARDS:

The paper documents, records, and files are maintained in file cabinets in the SOC's office suite. The file cabinets where these paper documents, files, and records are stored are controlled by on-site personnel when unlocked and locked when not in use. Access to the

SOC office suite is through a card-coded main door. Access to the file cabinets is restricted to authorized SOC supervisors, staff, and contractors, whose duties and responsibilities require use of the information.

The electronic records, files, and data are stored in the FCC computer network databases that are secured by limited access card readers. The computer servers themselves are password-protected. Access to the electronic files is restricted to authorized SOC supervisors, staff, and contractors, and to the Information Technology Center (ITC) staff and contractors, who maintain the FCC's computer network. Other FCC employees and contactors may be granted access on a ''need-to-know'' basis. The FCC's computer network databases are protected by the FCC's security protocols, which include controlled access, passwords, and other security features. A *PRIVACY WARNING NOTICE* appears on the monitor screen when records containing information on individuals are first displayed. Information resident on the SOC database servers is backed-up routinely onto magnetic media. Back-up tapes are stored on-site and at a secured, off-site location.

RETENTION AND DISPOSAL:

Records in the FCC Visitors Database are retained in accordance with General Records Schedule (GRS) 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 GRS 18, item 22a, approved by NARA. The records are disposed of in accordance with SOC disposal policies, as follows:

1. All returned day contractor cards will be reused on a daily basis.

2. Transaction data for all FCC Visitors Database cards will be stored using a secure medium and retained for one year in the SOC, which is locked and secured with an alarm system.

In accordance with Homeland Security Presidential Directive (HSPD–12), Personal Identity Verification (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 GRS 11, Item 4. PIV Cards are destroyed by burning in an approved Federal burn-facility.

SYSTEM MANAGER(S) AND ADDRESS:

Security Operations Center (SOC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

NOTIFICATION PROCEDURE:

Security Operations Center (SOC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

RECORD ACCESS PROCEDURES:

Security Operations Center (SOC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

CONTESTING RECORD PROCEDURES:

Security Operations Center (SOC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554.

RECORD SOURCE CATEGORIES:

The sources for information in this system are the visitors themselves and/or their agency or organizational sponsor(s) who have been invited to or have requested admittance to the FCC headquarters buildings and other FCC facilities for the visitors.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Federal Communications Commission.

Marlene H. Dortch,

Secretary, Office of the Secretary, Office of Managing Director.

[FR Doc. 2012–12949 Filed 5–29–12; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL DEPOSIT INSURANCE CORPORATION

Agency Information Collection Activities: Proposed Collection Renewal; Comment Request

AGENCY: Federal Deposit Insurance Corporation (FDIC).

ACTION: Notice and request for comment.

SUMMARY: The FDIC, as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to take this opportunity to comment on renewal of an existing information collection, as required by the Paperwork Reduction Act of 1995 (44 U.S.C. chapter 35). Currently, the FDIC is soliciting comments on renewal of the information collection described below.

DATES: Comments must be submitted on or before July 30, 2012.

ADDRESSES: Interested parties are invited to submit written comments to the FDIC by any of the following methods:

- *http://www.FDIC.gov/regulations/laws/federal/notices.html.*
- *Email: comments@fdic.gov.* Include the name of the collection in the subject line of the message.
- *Mail:* Leneta G. Gregorie (202–898–3719), Counsel, Room NYA–5050, Federal Deposit Insurance Corporation, 550 17th Street NW., Washington, DC 20429.
- *Hand Delivery:* Comments may be hand-delivered to the guard station at the rear of the 17th Street Building (located on F Street), on business days between 7:00 a.m. and 5:00 p.m.

All comments should refer to the relevant OMB control number. A copy of the comments may also be submitted to the OMB desk officer for the FDIC: Office of Information and Regulatory Affairs, Office of Management and Budget, New Executive Office Building, Washington, DC 20503.

FOR FURTHER INFORMATION CONTACT: Leneta G. Gregorie, at the FDIC address above.

SUPPLEMENTARY INFORMATION: Proposal to renew the following currently approved collection of information:

Title: Certification of Compliance with Mandatory Bars to Employment.

OMB Number: 3064–0121.

Form Number: FDIC 7300/06.

Frequency of Response: On occasion.

Affected Public: Business or other financial institutions.

Estimated Number of Respondents: 600.

Estimated Time per Response: 10 minutes.

Total Annual Burden: 100 hours.

General Description of Collection: Prior to an offer of employment, job applicants to the FDIC must sign a certification that they have not been convicted of a felony or been in other circumstances that prohibit person from becoming employed by or providing services to the FDIC.

Request for Comment

Comments are invited on: (a) Whether the collection of information is necessary for the proper performance of the FDIC's functions, including whether the information has practical utility; (b) the accuracy of the estimates of the burden of the information collection, including the validity of the methodology and assumptions used; (c) ways to enhance the quality, utility, and clarity of the information to be