Communications Supply Chain Through FCC Programs—Huawei Designation, PS Docket No. 19–351, Memorandum Opinion and Order, 35 FCC Rcd 14435 (2020); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs—ZTE Designation,* PS Docket No. 19–352, Memorandum Opinion and Order, DA 20–1399 (PSHSB rel. Nov. 24, 2020).

On December 10, 2020, the Commission adopted the *Second Report and Order* implementing the Secure Networks Act, which contained certain new information collection requirements. *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs,* WC Docket No. 18–89, Second Report and Order, 35 FCC Rcd 14284 (2020) (*Second Report and Order*). These requirements will allow the Commission to receive, review and make eligibility determinations and funding decisions on applications to participate in the Reimbursement Program that are filed by certain providers of advanced communications service. These new information collection requirements will also assist the Commission in processing funding disbursement requests and in monitoring and furthering compliance with applicable program requirements to protect against waste, fraud, and abuse.

On December 27, 2020, the President signed into law the Consolidated Appropriations Act, 2021, appropriating $1.9 billion to ''carry out'' the Reimbursement Program and amending the Reimbursement Program eligibility requirements to expand eligibility to include providers of advanced communications service with 10 million or fewer subscribers. *See* Public Law 116–260, Division N-Additional Coronavirus Response and Relief, Title IX-Broadband internet Access Service, §§ 901, 906, 134 Stat. 1182 (2020). The Commission has interpreted the term ''provider of advanced communications service'' to mean ''facilities-based providers, whether fixed or mobile, with a broadband connection to end users with at least 200 kbps in one direction.'' *Second Report and Order,* 35 FCC Rcd at 14332, para. 111. Participation in the Reimbursement Program is voluntary but compliance with the new information collection requirements is required to obtain Reimbursement Program support.

The Secure Networks Act requires all providers of advanced communications service to annually report, with exception, on whether they have purchased, rented, leased or otherwise obtained covered communications equipment or service on or after certain dates. 47 U.S.C. 1603(d)(2)(B). The *Second Report and Order* adopted a new information collection requirement to implement this statutory mandate. *See* Secure Networks Act § 5. If the provider certifies it does not have any covered equipment and services, then the provider is not required to subsequently file an annual report, unless it later obtains covered equipment and services. *Second Report and Order* at para. 215.

This submission is for new information collection requirements contained in the *Second Report and Order* adopted by the Commission on December 10, 2020. The new requirements are necessary for the creation of a $1.9 billion reimbursement program, as directed by Congress in the Secure Networks Act, as amended. This submission also covers a related information collection requirement necessitated by the Secure Networks Act and/or the *Second Report and Order* and proposes to eliminate a previously approved information collection requirement that is no longer necessary.

Federal Communications Commission.

Marlene Dortch,

Secretary, Office of the Secretary.

[FR Doc. 2021–16503 Filed 8–2–21; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL COMMUNICATIONS COMMISSION

[FR ID: 40816]

Privacy Act of 1974; System of Records

AGENCY: Federal Communications Commission.

ACTION: Notice of a modified System of Records.

SUMMARY: The Federal Communications Commission (FCC or Commission or Agency) has modified an existing system of records, FCC/PSHSB–1, FCC Emergency and Continuity Alerts and Contacts System (ECACS), subject to the Privacy Act of 1974, as amended. This action is necessary to meet the requirements of the Privacy Act to publish in the **Federal Register** notice of the existence and character of records maintained by the Agency. The FCC's Public Safety and Homeland Security Bureau (PSHSB) uses the information in ECACS to prepare for and coordinate crisis response activities wherever they occur in the United States and its territories. The FCC is modifying FCC/PSHSB–1 to add information it will use to alert the designated emergency contacts of Commission staff of an emergency involving the FCC or a staff member.

DATES: This action will become effective on August 3, 2021. Written comments on the system's routine uses are due by September 2, 2021. The routine uses in this action will become effective on September 2, 2021 unless written comments are received that require a contrary determination.

ADDRESSES: Send comments to Margaret Drake, at *privacy@fcc.gov,* or at Federal Communications Commission (FCC), 45 L Street, NE, Washington, DC 20554 at (202) 418–1707.

FOR FURTHER INFORMATION CONTACT: Margaret Drake, (202) 418–1707, or *privacy@fcc.gov* (and to obtain a copy of the Narrative Statement and the Supplementary Document, which includes details of the modifications to this system of records).

SUPPLEMENTARY INFORMATION: The FCC's Public Safety and Homeland Security Bureau (PSHSB) uses the information in ECACS to prepare for and coordinate crisis response activities wherever they occur in the United States and its territories. This notice serves to update and modify FCC/PSHSB–1 to add the personally identifiable information (PII) of Commission staff in the form of contact information and emergency contacts. The substantive changes and modifications to the previously published version of the FCC/PSHSB–1 system of records include:

1. Updating the Security Classification to follow OMB and FCC guidance.

2. Updating the Purposes for clarity and to include contacting the emergency contacts designated by FCC staff in case of an emergency involving a staff member.

3. Updating the Categories of Individuals to include emergency contacts designated by FCC staff.

4. Updating the Categories of Records to remove information that is no longer collected by this system and to include contact information for FCC employees' emergency contacts.

5. Updating the System Location to show the FCC's new headquarters address.

6. Adding two new Routine Uses: (1) FCC Program Management, to allow designated FCC staff to access the information in connection with the management and operation of a safe workplace, and (9) Non-Federal Personnel, to allow contractors performing or working on a contract for the Federal Government access to information in this system.

7. Revising three Routine Uses: (3) Law Enforcement and Investigation to include components of agencies; (5) Government-Wide Program Management and Oversight to remove references to federal agencies for which the Privacy Act already includes exceptions, see 5 U.S.C. 552a(6) and (10); and (10) Test Partners to include other federal agencies that will collaborate with the FCC on Wireless Emergency Alerts.

8. Removing one Routine Use: Contracted Third Parties and replacing it with a new Routine Use (9) Non-Federal Personnel.

The system of records is also updated to reflect various administrative changes related to the system address; administrative, technical, and physical safeguards; and updated notification, records access, and procedures to contest records.

SYSTEM NAME AND NUMBER:

FCC/PSHSB–1, FCC Emergency and Continuity Alerts and Contacts System (ECACS).

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Public Safety and Homeland Security Bureau (PSHSB), Federal Communications Commission (FCC), 45 L Street, NE, Washington, DC, 20554.

SYSTEM MANAGER(S):

Public Safety and Homeland Security Bureau (PSHSB), Federal Communications Commission (FCC).

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, April 3, 1984, as amended February 28, 2003 and June 26, 2006; Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Government Operations, October 21, 1998; Homeland Security Act of 2002, 6 U.S.C. 101 *et seq.,* November 25, 2002; National Security Presidential Directive 51/Homeland Security Presidential Directive 20, National Continuity Policy, May 9, 2007; National Communications System Directive 3–10, Minimum Requirements for Continuity Communications Capabilities, July 25, 2007; National Continuity Policy Implementation Plan, Homeland Security Council, August 2007; Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements, February 2008; Federal Continuity Directive 2, Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process, February 2008.

PURPOSE(S) OF THE SYSTEM:

The FCC uses the records in this system to:

1. Respond to and coordinate activities such as emergencies and crisis management actions, responses, and related functions, including contacting FCC staff and their designated emergency contacts and using an automated telephone, text, and email system;

2. Manage and maintain the contact and response system for FCC staff for coordinating Continuity of Operations Plan (COOP) actions and related functions;

3. Conduct voluntary surveys evaluating the effectiveness of Wireless Emergency Alerts (WEA) and other related emergency notification systems, functions, and activities.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals in this system include:

1. FCC staff and their designated emergency contacts.

2. Federal Government contacts; State, Tribal, Territorial, Local Government and private sector contacts; and individuals representing institutions, organizations, and other groups engaged in crisis management and emergency preparedness functions, activities, and actions.

3. FCC staff who are members of the Bureau and Office (B/O) Emergency Response Group (ERG), Devolution Emergency Response Group (DERG), and FCC and B/O lines of succession.

4. Individuals who volunteer to participate in PSHSB surveys for WEA.

CATEGORIES OF RECORDS IN THE SYSTEM:

The records in this system include personal and business contact information, such as phone number, fax number, email address, physical address. Records also include survey information, such as the individual respondents' identification numbers, email addresses, street addresses (street, city, state, and zip code) at the location that the individual responds to the survey, and other information that PSHSB will collect, such as the type of device, operating system, and wireless service provider.

RECORD SOURCE CATEGORIES:

FCC employees and contractors, Federal Government, State, Tribal, Territorial, Local Government, and private sector contacts representing institutions and organizations with crisis management and emergency preparedness functions, as well as survey respondents' inputs transmitted through their wireless devices, or through other means of communication.

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

In addition to those disclosures generally permitted under section 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside the FCC, as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows.

1. FCC Program Management—A record from this system may be accessed and used by the FCC's Office of Managing Director or supervisory staff in their duties associated with the management and operation of a safe workplace. This information may be used to notify staff and their designated emergency contacts of an emergency situation involving the FCC or a staff member.

2. Adjudication and Litigation—To disclose information to the Department of Justice (DOJ), or to a court or adjudicative body before which the FCC is authorized to appear, when: (a) The FCC or any component thereof; or (b) any employee of the FCC in his or her official capacity; or (c) any employee of the FCC in his or her individual capacity where the DOJ or the FCC have agreed to represent the employee; or (d) the United States is a party to litigation or have an interest in such litigation, and the use of such records by the DOJ or the FCC is deemed by the FCC to be relevant and necessary to the litigation.

3. Law Enforcement and Investigation—To disclose pertinent information to the appropriate Federal, State, and/or local agency, or component of an agency, such as the FCC's Enforcement Bureau, responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where the FCC becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.

4. Congressional Inquiries—To provide information to a Congressional office from the record of an individual in response to an inquiry from that Congressional office made at the written request of that individual.

5. Government-Wide Program Management and Oversight—To disclose information to the Department of Justice (DOJ) to obtain that department's advice regarding

disclosure obligations under the Freedom of Information Act (FOIA); or to the Office of Management and Budget (OMB) to obtain that office's advice regarding obligations under the Privacy Act.

6. Labor Relations—To officials of labor organizations recognized under 5 U.S.C. 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.

7. Breach Notification—To appropriate agencies, entities, and persons when (a) the Commission suspects or has confirmed that there has been a breach of the system of records; (b) the Commission has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Commission (including its information systems, programs, and operations), the Federal Government, or national security; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with Commission efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

8. Assistance to Federal Agencies and Entities—To another Federal agency or Federal entity, when the Commission determines that information from this system is reasonably necessary to assist the recipient agency or entity in: (a) Responding to a suspected or confirmed breach or (b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, program, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

9. Non-Federal Personnel—To disclose information to non-federal personnel, including contractors, 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.

10. Test Partners—To PSHSB's test partner entities, including other federal agencies, who help plan, conduct, and analyze the results of tests used to evaluate the effectiveness of WEA.

REPORTING TO A CONSUMER REPORTING AGENCY:

In addition to the routine uses listed above, the Commission may share information from this system of records with a consumer reporting agency regarding an individual who has not paid a valid and overdue debt owed to the Commission, following the procedures set out in the Debt Collection Act, 31 U.S.C. 3711(e).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Information in ECACS consists of electronic data, files, and records, which are housed in the FCC's computer network databases, and paper documents, files, and records, which are stored in file cabinets in the PSHSB office suite.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information in the Emergency Contacts and the COOP Contacts databases is retrieved by searching any field in the respective database(s).

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The FCC maintains and disposes of these records in accordance with the requirements of the General Records Schedules (GRS) issued by the National Archives and Records Administration (NARA) as follows:

GRS 5.3, Disposition Authorities:

Item 010: DAA–GRS–2016–0004–0001: Continuity planning and related emergency planning files; and

Item 020: DAA–GRS–2016–0004–0002: Employee emergency contact information.

GRS 4.1, Disposition Authority: Item 030: DAA–GRS–2013–0002–0008: Vital or essential records program records.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

1. The electronic records, data, and files are stored within FCC accreditation boundaries and maintained in a database housed in the FCC computer network databases. Access to the electronic files is restricted to authorized Commission employees and contractors; and to IT staff, contractors, and vendors who maintain the IT networks and services. Other FCC employees and contractors may be granted access on a need-to-know basis. The FCC's electronic files and records protected by the FCC and third-party privacy safeguards, a comprehensive and dynamic set of IT safety and security protocols and features that are designed to meet all Federal privacy standards, including those required by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Information Security Modernization Act of 2014 (FISMA).

2. There are a limited number of paper documents, files, and records, which are stored in file cabinets in the FCC Operations Center and continuity sites. These cabinets are locked when not in use and/or at the end of the business day. All access points for these locations are monitored.

3. PSHSB's Test Partners and contractors will not have direct access to the FCC's computer network or information systems; however, PSHSB will provide the Test Partners data necessary to evaluate the effectiveness of WEA. The Test Partners will be required to implement privacy safeguards against the disclosure of electronic data and paper document files provided by the FCC.

RECORD ACCESS PROCEDURES:

Individuals wishing to request access to and/or amendment of records about them should follow the Notification Procedure below.

CONTESTING RECORD PROCEDURES:

Individuals wishing to request an amendment of records about them should follow the Notification Procedure below.

NOTIFICATION PROCEDURES:

Individuals wishing to determine whether this system of records contains information about themselves may do so by writing *Privacy@fcc.gov*. Individuals requesting access must also comply with the FCC's Privacy Act regulations regarding verification of identity to gain access to records as required under 47 CFR part 0, subpart E.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

The FCC last gave full notice of this system of records, FCC/PSHSB–1, by publication in the **Federal Register** on April 24, 2020 (85 FR 23024).

Federal Communications Commission.

Marlene Dortch,

Secretary.

[FR Doc. 2021–16511 Filed 8–2–21; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL COMMUNICATIONS COMMISSION

[OMB 3060–1086 and OMB 3060–1216; FR ID 41065]

Information Collections Being Reviewed by the Federal Communications Commission

AGENCY: Federal Communications Commission.

ACTION: Notice and request for comments.