and Resources Research, National Institutes of Health, HHS)

Dated: July 24, 2012.

Jennifer S. Spaeth,

Director, Office of Federal Advisory Committee Policy.

[FR Doc. 2012–18477 Filed 7–27–12; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2012–0001]

Critical Infrastructure Private Sector Clearance Program Request

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: 30-day notice and request for comments;

Reinstatement, with change, of a previously approved collection.

SUMMARY: The Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), Office of Infrastructure Protection (IP) will submit the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995 (Pub. L. 104–13, 44 U.S.C. Chapter 35). NPPD is soliciting comments concerning Reinstatement, with change, of a previously approved ICR for the Critical Infrastructure Private Sector Clearance Program (PSCP). DHS previously published this ICR in the **Federal Register** on April 12, 2012, for a 60-day public comment period. DHS received no comments. The purpose of this notice is to allow an additional 30 days for public comments.

DATES: Comments are encouraged and will be accepted until August 29, 2012. This process is conducted in accordance with 5 CFR 1320.10.

ADDRESSES: Interested persons are invited to submit written comments on the proposed information collection to the Office of Information and Regulatory Affairs, OMB. Comments should be addressed to OMB Desk Officer, DHS, Office of Civil Rights and Civil Liberties. Comments must be identified by DHS–2012–0001 and may be submitted by one of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.*
- *Email: oira_submission@omb.eop.gov*. Include the docket number in the subject line of the message.
- *Fax:* (202) 395–5806.

Instructions: All submissions received must include the words ''Department of Homeland Security'' and the docket number for this action. Comments received will be posted without alteration at *http://www.regulations.gov*, including any personal information provided.

OMB is particularly interested in comments that:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
2. Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;
3. Enhance the quality, utility, and clarity of the information to be collected; and
4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

FOR FURTHER INFORMATION CONTACT: Monika Junker, DHS/NPPD/IP, *monika.junker@dhs.gov*, (703) 235–8229.

SUPPLEMENTARY INFORMATION: PSCP sponsors clearances for private sector partners who are responsible for critical infrastructure protection but would not otherwise be eligible for a clearance under Executive Order 12829. These partners are subject matter experts within specific industries and sectors. The PSCP requires individuals to complete a clearance request form that initiates the clearance process. DHS Sector Specialists or Protective Security Advisors email the form to the individual who then emails back the completed form, minus their date and place of birth and social security number. The clearance request form is signed by both the Federal official who nominated the applicant and the Assistant Secretary for Infrastructure Protection. Upon approval to process, the PSCP Administrator contacts the nominee to obtain the social security number, date and place of birth, and will then enter this data into e-QIP—Office of Personnel Management's secure portal for investigation processing. Once the data is entered in e-QIP, the applicant can complete the online security questionnaire. The PSCP maintains all applicants' information in the Master Roster, which contains all the information found on the clearance request form in addition to their clearance information (date granted, level of clearance, date non-disclosure agreements signed, and type/date of investigation). The Administrator of the Master Roster maintains the information to track clearance processing and investigation information and to have the most current contact information for the participants from each sector.

Analysis

Agency: Department of Homeland Security, National Protection and Programs Directorate, Office of Infrastructure Protection.

Title: Critical Infrastructure Private Sector Clearance Program.

OMB Number: 1670–0013.

Frequency: Once.

Affected Public: Designated private sector employees of critical infrastructure entities or organizations.

Number of Respondents: 450 (estimate).

Estimated Time Per Respondent: 10 minutes.

Total Burden Hours: 75.

Total Burden Cost (capital/startup): $0.

Total Recordkeeping Burden: $0.

Total Burden Cost (operating/maintaining): $0.

Dated: July 24, 2012.

Scott Libby,

Acting Chief Information Officer, National Protection and Programs Directorate, Department of Homeland Security.

[FR Doc. 2012–18546 Filed 7–27–12; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2012–0037]

President's National Security Telecommunications Advisory Committee

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: Committee Management; Notice of an Open Federal Advisory Committee Teleconference.

SUMMARY: The President's National Security Telecommunications Advisory Committee (NSTAC) will meet on Thursday, August 16, 2012, via a conference call. The meeting will be open to the public.

DATES: The NSTAC will meet Thursday, August 16, 2012, from 2:00 p.m. to 3:15 p.m. Please note that the meeting may close early if the committee has completed its business.

ADDRESSES: The meeting will be held via a conference call. For access to the

conference bridge, contact Ms. Deirdre Gallop-Anderson by email at *deirdre.gallop-anderson@dhs.gov* by 5:00 p.m. on August 9, 2012.

To facilitate public participation, we are inviting public comment on the issues to be considered by the committee as listed in the ''Supplementary Information'' section below. Documents associated with the issues to be discussed during the conference will be available at *www.ncs.gov/nstac* for review by August 10, 2012. Written comments must be received by the NSTAC Designated Federal Officer no later than August 30, 2012 and may be submitted by any *one* of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov*. Follow the instructions for submitting written comments.
- *Email: NSTAC@hq.dhs.gov*. Include the docket number in the subject line of the email message.
- *Fax:* (703) 235–4981.
- *Mail:* Alternate Designated Federal Officer, National Communications System, National Protection and Programs Directorate, Department of Homeland Security, 245 Murray Lane, Mail Stop 0615, Arlington, VA 20598–0615.

Instructions: All submissions received must include the words ''Department of Homeland Security'' and the docket number for this action. Comments received will be posted without alteration at *www.regulations.gov*, including any personal information provided.

Docket: For access to the docket, including all documents and comments received by the NSTAC, go to *www.regulations.gov*.

A public comment period will be held during the meeting on August 16, 2012, from 2:55 p.m. to 3:10 p.m. Speakers who wish to participate in the public comment period must register in advance no later than 5:00 p.m. on August 9, 2012, by emailing Deirdre Gallop-Anderson at *deirdre.gallop-anderson@dhs.gov*. Speakers are requested to limit their comments to three minutes and will speak in order of registration as time permits. Please note that the public comment period may end before the time indicated, following the last call for comments.

FOR FURTHER INFORMATION CONTACT: Allen F. Woodhouse, NSTAC Alternate Designated Federal Officer, Department of Homeland Security, telephone (703) 235–4900.

SUPPLEMENTARY INFORMATION: Notice of this meeting is given under the Federal Advisory Committee Act, 5 U.S.C. App. (Pub. L. 92–463). The NSTAC advises the President on matters related to national security and emergency preparedness telecommunications policy.

Agenda: The NSTAC members will receive an update on progress made to date by the Nationwide Public Safety Broadband Network (NPSBN) Research Subcommittee. The NPSBN Research Subcommittee is focusing on what National Security Emergency Preparedness (NS/EP) policy changes should be considered in order to: (1) Facilitate priority access that may be required across the diverse community of potential NPSBN users, particularly during NS/EP situations; (2) support NPSBN access, interoperability, security, reliability, and resiliency; and (3) help ensure the deployment and evolution of the NPSBN is in such a manner that accounts for each state and local jurisdiction's diverse capabilities, while helping to ensure scalability to the national level.

Next, NSTAC members will discuss the findings of their review of the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC). During the NSTAC meeting on May 15, 2012, the National Security Staff asked the NSTAC to conduct a review of the NCCIC to determine if it is operating in ways consistent with the NSTAC's proposed Joint Collaboration Center that the NSTAC envisioned in its 2009 Cybersecurity Collaboration Report.

The NSTAC, in coordination with senior leaders from the White House and DHS, will also address potential NSTAC taskings such as the National Security Staff's request for the NSTAC to examine how commercial off-the-shelf technologies and private sector best practices can be used to secure unclassified communications between and among Federal civilian departments and agencies.

Additionally, there will be a discussion regarding whether further study is warranted of the NSTAC's recommendation to develop a separate ''out-of-band'' data network supporting communications among carriers, Internet service providers, vendors, and additional critical infrastructure owners and operators during a severe cyber incident that renders the Internet unusable.

Dated: July 23, 2012.

Michael Echols,

Alternate Designated Federal Officer for the NSTAC.

[FR Doc. 2012–18536 Filed 7–27–12; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2012–0045]

Privacy Act of 1974; Department of Homeland Security U.S. Customs and Border Protection-DHS/CBP–009 Electronic System for Travel Authorization (ESTA) System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to update and reissue a current DHS system of records titled, ''Department of Homeland Security/U.S. Customs and Border Protection-DHS/CBP–009 Electronic System for Travel Authorization (ESTA) System of Records.'' This system collects and maintains a record of nonimmigrant aliens seeking to travel to the United States under the Visa Waiver Program. The system is used to determine whether the applicant is eligible to travel to the United States under the Visa Waiver Program by vetting the application information against selected security and law enforcement databases using U.S. Customs and Border Protection (CBP) TECS and the Automated Targeting System (ATS). In addition, ATS retains a copy of ESTA application data to identify potential high-risk ESTA applicants. DHS/CBP is updating this system of records notice to clarify the categories of individuals and remove unnecessary language, add the Internet Protocol address associated with the submitted ESTA application as a category of records, provide more specific legal authorities, clarify the purposes to include the identification of high-risk applicants, include an additional routine use for judicial proceedings and update and clarify other routine uses, clarify the retention of records in ESTA and the Nonimmigrant Information System (DHS/CBP–016—Nonimmigrant Information System December 19, 2008 73 FR 77739), update the notification procedures to explain the extension of access procedures to international travelers, allow limited direct access and amendment of ESTA application data, and add the CPB access request address; eliminate unnecessary language from the record source categories, and clarify which exemptions will be used for which provisions of the Privacy Act.