AZ 85040, 602–438–8507/800–279–0027

STERLING Reference Laboratories, 2617 East L Street, Tacoma, Washington 98421, 800–442–0438

US Army Forensic Toxicology Drug Testing Laboratory, 2490 Wilson St., Fort George G. Meade, MD 20755–5235, 301–677–7085

Summer King,

Statistician.

[FR Doc. 2014–26131 Filed 11–3–14; 8:45 am]

BILLING CODE 4160–20–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2014–0048]

President's National Security Telecommunications Advisory Committee

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: Committee Management; Notice of Partially Closed Federal Advisory Committee Meeting.

SUMMARY: The President's National Security Telecommunications Advisory Committee (NSTAC) will meet on Wednesday, November 19, 2014, in Washington DC The meeting will be partially closed to the public.

DATES: The NSTAC will meet in a closed session on Wednesday, November 19, 2014, from 8:30 a.m. to 10:30 a.m. and in an open session on Wednesday, November 19, 2014, from 10:40 a.m. to 2:40 p.m.

ADDRESSES: The open, public session will be held at the Department of Homeland Security Immigration and Customs Enforcement facility, 500 12th Street SW., Washington DC, and will begin at 10:40 a.m. For information on facilities or services for individuals with disabilities, to request special assistance at the meeting, or to attend in person contact *nstac@dhs.gov* as soon as possible.

We are inviting public comment on the issues the NSTAC will consider, as listed in the **SUPPLEMENTARY INFORMATION** section below. Associated briefing materials that will be discussed at the meeting will be available at *www.dhs.gov/nstac* for review as of November 5, 2014. Comments must be identified by docket number DHS–2014–0048 and may be submitted by *one* of the following methods:

- Federal eRulemaking Portal: *http://www.regulations.gov.* Follow the instructions for submitting comments.
- Email: *NSTAC@dhs.gov.* Include the docket number in the subject line of the message.
- Fax: 703–235–5962, Attn: Sandy Benevides.
- Mail: Designated Federal Officer, National Security Telecommunications Advisory Committee, 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 *http://www.regulations.gov,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received by the NSTAC, go to *http://www.regulations.gov,* referencing docket number DHS–2014–0048.

A public comment period will be held during the open portion of the meeting on Wednesday, November 19, 2014, from 1:35 p.m. to 2:05 p.m., and speakers are requested to limit their comments to three minutes. Please note that the public comment period may end before the time indicated, following the last call for comments. Contact Sandy Benevides at 703–235–5408 or *Sandra.Benevides@dhs.gov* to register as a speaker by close of business on November 17, 2014. Speakers will be accommodated in order of registration within the constraints of the time allotted to public comment.

FOR FURTHER INFORMATION CONTACT: Helen Jackson, NSTAC Designated Federal Officer, Department of Homeland Security, telephone (703) 235–5321 or *Helen.Jackson@dhs.gov.*

SUPPLEMENTARY INFORMATION: Notice of this meeting is given under the *Federal Advisory Committee Act,* 5 U.S.C. Appendix. The NSTAC advises the President on matters related to national security and emergency preparedness (NS/EP) telecommunications policy.

Agenda: The committee will meet in the open session to engage in an update of the Federal Communications Commission's current priorities; a discussion of the Department of Justice's Anti-Trust Guidelines; the current priorities and accomplishments of the First Responder Network Authority; a panel discussion of the interdependencies between the Communications and Electric Power Sector. The NSTAC members will deliberate and vote on the *NSTAC Report to the President on the Cybersecurity Implications of the Internet of Things* and the *NSTAC Report to the President on Information and Communications Technology Mobilization.* Both reports will be available at *www.dhs.gov/nstac* as of November 5, 2014.

The NSTAC will meet in a closed session to hear a classified briefing regarding emerging threats to the communications infrastructure and to discuss the potential future NSTAC study topics.

Basis for Closure: In accordance with 5 U.S.C. § 552b(c), *The Government in the Sunshine Act,* it has been determined that two agenda items require closure as the disclosure of the information would not be in the public interest.

The first of these agenda items, the classified briefing, will provide members with information on nation-state capabilities and strategic threats. Such threats target national communications infrastructure and impact industry's long-term competitiveness and growth, as well as the Government's ability to mitigate threats. Malicious actors continue to advance their techniques to exploit critical infrastructure networks and poses serious challenges for the communications sector. Disclosure of these threats would provide criminals who wish to intrude into commercial and Government networks with information on potential vulnerabilities and mitigation techniques, also weakening existing cybersecurity defense tactics. This briefing will be classified at the top secret level, thereby exempting disclosure of the content by statute. Therefore, this portion of the meeting is required to be closed pursuant to 5 U.S.C. § 552b(c)(1)(A).

The second agenda item, the discussion of potential NSTAC study topics, will address areas of critical cybersecurity vulnerabilities and priorities for Government. Government officials will share data with NSTAC members on initiatives, assessments, and future security requirements across public and private networks. The data to be shared includes specific vulnerabilities within cyberspace that affect the Nation's communications and information technology infrastructures and proposed mitigation strategies. Disclosure of this information to the public would provide criminals with an incentive to focus on these vulnerabilities to increase attacks on our cyber and communications networks. Therefore, this portion of the meeting is likely to significantly frustrate implementation of proposed DHS actions and is required to be closed pursuant to 5 U.S.C. 552b(c)(9)(B).

Dated: October 28, 2014.

Helen Jackson,

Designated Federal Officer for the NSTAC.

[FR Doc. 2014–26097 Filed 11–3–14; 8:45 am]

BILLING CODE P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2014–0057]

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: Department of Homeland Security, Privacy Office.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) proposes to update 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 of records allows the U.S. Customs and Border Protection (CBP) at DHS to collect and maintain records on nonimmigrant aliens seeking to travel to the United States under the Visa Waiver Program and other persons, including U.S. citizens and lawful permanent residents, whose name is provided to DHS as part of a nonimmigrant alien's ESTA application. The system is used to determine whether the applicant is eligible to travel to and enter the United States under the Visa Waiver Program by vetting the ESTA application information against selected security and law enforcement databases at DHS, including but not limited to the use of CBP's TECS (not an acronym) and the Automated Targeting System (ATS). In addition, ATS retains a copy of ESTA application data to identify ESTA applicants who may pose a security risk to the United States. ATS maintains copies of key elements of certain databases in order to minimize the impact of processing searches on the operational systems and to act as a backup for certain operational systems. DHS may also vet ESTA application information against security and law enforcement databases at other Federal agencies to enhance DHS's ability to determine whether the applicant poses a security risk to the United States and is eligible to travel to and enter the United States under the Visa Waiver Program. The results of this vetting may inform DHS's assessment of whether the applicant's travel poses a law enforcement or security risk and whether the application should be approved.

As part of the Department's ongoing effort to promote transparency regarding its collection of information, DHS/CBP is updating: (1) The categories of individuals covered by the system, and (2) categories of records in the system to include revised eligibility questions and additional data elements collected on the ESTA application. DHS issued a Final Rule to exempt this system of records from certain provisions of the Privacy Act on August 31, 2009 (74 FR 45070). These regulations remain in effect.

Furthermore, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. This updated system will be included in DHS's inventory of systems of records, located on the DHS Web site at *http://www.dhs.gov/system-records-notices-sorns.*

DATES: This updated system will be effective upon the public display of this notice. Although this system is effective upon publication, DHS will accept and consider comments from the public and evaluate the need for any revisions to this notice.

ADDRESSES: You may submit comments on this notice, including the applicability of the exemptions set forth in the August 31, 2009 Final Rule (74 FR 45070) to the new categories of individuals and categories of records, identified by docket number DHS–2014–0057, by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 202–343–4010.
- *Mail:* Karen L. Neuman, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received, please visit *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: John Connors, (202) 344–1610, CBP Privacy Officer, Privacy and Diversity Office, 1300 Pennsylvania Ave. NW., Washington, DC 20229. For privacy questions, please contact: Karen L. Neuman, (202) 343–1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is updating a current DHS system of records titled, ''DHS/CBP–009 Electronic System for Travel Authorization (ESTA) System of Records.''

In the wake of the tragedy of September 11, 2001, Congress enacted the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110–53. Section 711 of that Act sought to address the security vulnerabilities associated with Visa Waiver Program (VWP) travelers not being subject to the same degree of screening as other international visitors. As a result, section 711 requires DHS to develop and implement a fully automated electronic travel authorization system to collect biographical and other information necessary to evaluate the security risks and eligibility of an applicant to travel to the United States under the VWP. The VWP is a travel facilitation program that has evolved since the terrorist attack on the Nation on September 11, 2001, to include more robust security standards that are designed to prevent terrorists and other criminal actors from exploiting the Program to enter the country.

ESTA is a Web-based system that DHS/CBP developed in 2008 to determine the eligibility of foreign nationals to travel by air or sea to the United States under the VWP. Applicants submit biographic information and answer eligibility questions using the ESTA Web site. CBP uses the information submitted to ESTA to make a determination regarding whether the applicant's intended travel poses a law enforcement or security risk. CBP vets the ESTA applicant information against selected security and law enforcement databases, including the use of TECS and the Automated Targeting System (ATS). ATS also retains a copy of ESTA application data to identify ESTA applicants who may pose a security risk to the United States. ATS maintains copies of key elements of certain databases in order to minimize the