visitors for screening in FAMS and in the Classified Local Area Network (C–LAN) access database for twenty years.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

DHS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and consequently those of the Judicial Redress Act if applicable. However, DHS will consider individual requests to determine whether or not information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and Chief Freedom of Information Act (FOIA) Officer, whose contact information can be found at *http://www.dhs.gov/foia* under ''Contacts Information.'' If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief FOIA Officer, Department of Homeland Security, Washington, DC 20528–0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, *http://www.dhs.gov/foia* or 1–866–431–0486. In addition, the individual should:

- Explain why you believe the Department would have information on him/her;
- Identify which component(s) of the Department the individual believes may have the information about him/her;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

If an individual's request is seeking records pertaining to another living individual, the first individual must include a statement from the second individual certifying his/her agreement for the first individual to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES:

For records covered by the Privacy Act or covered JRA records, see ''Record Access Procedures'' above.

NOTIFICATION PROCEDURES:

See ''Record Access Procedures'' above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). When this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

HISTORY:

DHS/ALL–039 Foreign Access Management System of Records, 82 FR 34971 (July 27, 2017).

Philip S. Kaplan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2018–09196 Filed 4–30–18; 8:45 am]

BILLING CODE 9110–9B–P

DEPARTMENT OF HOMELAND SECURITY

[Docket ID DHS–2018–0019]

The President's National Security Telecommunications Advisory Committee

AGENCY: National Protection and Programs Directorate, Department of Homeland Security.

ACTION: Committee management; notice of federal advisory committee meeting.

SUMMARY: The President's National Security Telecommunications Advisory Committee (NSTAC) will meet on Thursday, May 17, 2018, in Washington, DC. The meeting will be partially closed to the public.

DATES: The NSTAC will meet on Thursday, May 17, 2018, from 9:30 a.m. to 3:30 p.m. Eastern Time (ET). Please note that the meeting may close early if the committee has completed its business.

ADDRESSES: The May 2018 NSTAC Meeting will be held at the Eisenhower Executive Office Building, Washington, DC. Due to limited seating, requests to attend in person will be accepted and processed in the order in which they are received. The meeting's proceedings will also be available via Webcast at *http://www.whitehouse.gov/live,* for those who cannot attend in person. Individuals who intend to participate in the meeting will need to register by sending an email to *NSTAC@hq.dhs.gov* by 5:00 p.m. ET on Friday, May 11, 2018. For information on facilities or services for individuals with disabilities, or to request special assistance at the meeting, or to attend in person, contact *NSTAC@hq.dhs.gov* as soon as possible. Members of the public are invited to provide comment on the issues that will be considered by the committee as listed in the **SUPPLEMENTARY INFORMATION** section below. Associated briefing materials that participants may discuss during the meeting will be available at *www.dhs.gov/nstac* for review as of Friday, May 4, 2018. Comments may be submitted at any time and must be identified by docket number DHS–2018–0019. Comments may be submitted by one of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Please follow the instructions for submitting written comments.
- *Email: NSTAC@hq.dhs.gov.* Include the docket number DHS–2018–0019 in the subject line of the email.

• *Fax:* (703) 705–6190, ATTN: Sandy Benevides.

• *Mail:* Helen Jackson, Designated Federal Officer, Stakeholder Engagement and Critical Infrastructure Resilience Division, National Protection and Programs Directorate, Department of Homeland Security, 245 Murray Lane, Mail Stop 0612, Arlington, VA 20598–0612.

Instructions: All submissions received must include the words ''Department of Homeland Security'' and the docket number DHS–2018–0019. Comments received will be posted without alteration at *www.regulations.gov,* including any personal information provided.

Docket: For access to the docket and comments received by the NSTAC, please go to *www.regulations.gov* and enter docket number DHS–2018–0019.

A public comment period will be held during the meeting on Thursday, May 17, 2018, from 2:40 p.m. to 3:00 p.m. ET. Speakers who wish to participate in the public comment period must register in advance by no later than Friday, May 11, 2018, at 5:00 p.m. ET by emailing *NSTAC@hq.dhs.gov.* Speakers are requested to limit their comments to three minutes and will speak in order of registration. Please note that the public comment period may end before the time indicated, following the last request for comments.

FOR FURTHER INFORMATION CONTACT: Helen Jackson, NSTAC Designated Federal Officer, Department of Homeland Security, (703) 705–6276 (telephone) or *helen.jackson@hq.dhs.gov* (email).

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

Agenda: The committee will meet in an open session on May 17, 2018, receive remarks from Department of Homeland Security (DHS) leadership and other senior Government officials regarding the Government's current cybersecurity initiatives and NS/EP priorities. The meeting will include a keynote address and a debate consisting of great thinkers in cybersecurity. NSTAC members will also receive a status update on the NSTAC Cybersecurity Moonshot Subcommittee's examination of concepts related to a Cybersecurity Moonshot, which has two primary objectives: (1) Defining an ambitious but achievable outcome-focused end goal for the cybersecurity environment; and (2) defining the structure and process necessary to successfully execute against the identified end goal.

The committee will also meet in a closed session to receive a classified briefing regarding cybersecurity threats and discuss future studies based on the Government's NS/EP priorities and perceived vulnerabilities.

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 discussed would not be in the public interest. The first of these agenda items, the classified briefing, will provide members with a cybersecurity threat briefing on vulnerabilities related to the communications infrastructure. Disclosure of these threats would provide criminals who seek to compromise commercial and Government networks with information on potential vulnerabilities and mitigation techniques, weakening the Nation's cybersecurity posture. This briefing will be classified at the top secret/sensitive compartmented information 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) & (B). The second agenda item, a 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 sector networks. The information will include specific vulnerabilities within cyberspace that affect the United States' information and communications 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 the Nation's critical infrastructure and communications networks. As disclosure of this portion of the meeting is likely to significantly frustrate implementation of proposed DHS actions, it is required to be closed pursuant to 5 U.S.C. 552b(c)(9)(B).

Helen Jackson,

Designated Federal Officer for the NSTAC.

[FR Doc. 2018–09234 Filed 4–30–18; 8:45 am]

BILLING CODE 9110–9X–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2018–0001]

Privacy Act of 1974; System of Records

AGENCY: U.S. Citizenship and Immigration Services, Department of Homeland Security.

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security/U.S. Citizenship and Immigration Services proposes to modify and reissue a current Department of Homeland Security system of records, Department of Homeland Security/U.S. Citizenship and Immigration Services—012, ''United States Citizenship and Immigration Services—012 Citizenship and Immigration Data Repository.'' The Citizenship and Immigration Data Repository is a mirror copy of the U.S. Citizenship and Immigration Services' major immigrant and non-immigrant unclassified benefits databases combined into a single user interface and presented in an updated searchable format on the classified network. This system of records is being updated to clarify categories of records, add the Password Issuance and Control System Identification Number as a retrievable data element, update the retention period for records maintained in CIDR; update routine use E and add routine use F to comply with new policy contained in Office of Management and Budget Memorandum M–17–12; update the record source categories, update the system manager information; and explain limitations set by law to the exemptions claimed for this system. Furthermore, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice and to provide further transparency as to how the system is used, in alignment with the recently republished Privacy Impact Assessment, DHS/USCIS/PIA–031(a) Citizenship & Immigration Data Repository. This modified system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before May 31, 2018. This modified system will be effective upon publication. Modified routine use E and new routine use F will be effective May 31, 2018.

ADDRESSES: You may submit comments, identified by docket number DHS–2018–0001 by one of the following methods: