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–DHS–2015–0056.

A public comment period will be held during the open portion of the meeting on Tuesday, November 10, 2015, from 1:55 p.m. to 2:10 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. Please contact *Helen.Jackson@dhs.gov* to register as a speaker by close of business on November 8, 2015. 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 (Pub. L. 92–463). 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 receive an update on current engagement activities between the NSTAC and the NS/EP Communications Executive Committee. The NSTAC will also hold a panel discussion on high performance computing and big data convergence, focusing on public private and cross agency collaboration and the predictive analytics capabilities of big data. The NSTAC will receive brief remarks on the U.S. Department of Commerce's (DOC) progress in promoting Government's cybersecurity efforts since the adoption of the National Institute of Standards and Technology Cybersecurity Framework, the process and approach under which the DOC continues to seek partners for its cybersecurity initiatives, and how private sector participation helps to promote the DOC's cybersecurity efforts. In addition, the NSTAC will receive an update on the work of the NSTAC's examination of big data analytics. The meeting agenda will be available at *www.dhs.gov/nstac* as of October 27, 2015.

The NSTAC will meet in a closed session to hear a classified briefing regarding current cyber threats against the communications infrastructure, and to discuss 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 current threats against the communications infrastructure. 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 20, 2015.

Helen Jackson,

Designated Federal Officer for the NSTAC.

[FR Doc. 2015–27101 Filed 10–23–15; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2015–0017]

Notice of Public Meeting Regarding Standards for Information Sharing and Analysis Organizations

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

ACTION: Notice of public meeting.

SUMMARY: In accordance with EO 13691, DHS has entered into a cooperative agreement with a non-governmental ISAO Standards Organization led by the University of Texas at San Antonio with support from the Logistics Management Institute (LMI) and the Retail Cyber Intelligence Sharing Center (R–CISC). This Notice announces the ISAO Standards Organization's initial public meeting on November 9, 2015 to discuss Standards for the development of ISAOs, as related to Executive Order 13691, ''Promoting Private Sector Cybersecurity Information Sharing'' of February 13, 2015. This meeting builds off of the workshops held on June 9, 2015 at the Volpe Center in Cambridge, MA; and July 30, 2015 at San Jose State University in San Jose, CA.

DATES: The meeting will be held on November 9, 2015, from 8:00 a.m. to 5:00 p.m. The meeting may conclude before the allotted time if all matters for discussion have been addressed.

ADDRESSES: The meeting location is LMI Headquarters at 7940 Jones Branch Drive, Tysons, VA 22102. *See Supplementary Information section for the address to submit written or electronic comments.*

SUPPLEMENTARY INFORMATION: Executive Order 13691 can be found at: *https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.*

FOR FURTHER INFORMATION CONTACT: If you have questions concerning the meeting, please contact *ISAO@lmi.org.*

Background and Purpose

On February 13, 2015, President Obama signed Executive Order 13691 intended to enable and facilitate ''private companies, nonprofit organizations, and executive departments and agencies . . . to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.''

At the Standards Organization's initial public meeting, they intend to review the results of previous DHS-hosted public workshops, and share a proposed standards framework and standards development process. In addition, they will solicit suggestions on existing standards, guidelines, and best practices that can be shared as provisional guidance until formal ISAO standards are established. Minutes from

this meeting will be made available to the public.

Information on Service for Individuals With Disabilities

For information on facilities or services for individuals with disabilities or to request special assistance at the public meeting, contact *ISAO@lmi.org* and write ''Special Assistance'' in the subject box or contact the meeting coordinator at the **FOR FURTHER INFORMATION CONTACT** section of this notice.

Meeting Details

Members of the public may attend this meeting by RSVP only up to the seating capacity of the room. The Breakout Panels that take place in the LMI Conference Facility will be audio recorded. The audio recordings will be made available on the DHS ISAO Web page, *DHS.gov/ISAO.* A valid government-issued photo identification (for example, a driver's license) will be required for entrance to the meeting space. Those who plan to attend should RSVP through the link provided on the ISAO Web page *DHS.gov/ISAO* or at LMI's registration page *www.lmi.org/ISAO-Registration* no later than 5 days prior to the meeting. Requests made after November 4, 2015 might not be able to be accommodated.

DHS and the ISAO Standards Organization encourages you to participate in this meeting by submitting comments to the ISAO inbox (*ISAO@lmi.org*), commenting orally, or submitting written comments to the DHS personnel attending the meeting who are identified to receive them.

Submitting Written Comments

You may also submit written comments to the docket using any one of the following methods:

(1) *Federal eRulemaking Portal: http://www.regulations.gov.* Although comments are being submitted to the Federal eRulemaking Portal, this is a tool to provide transparency to the general public, not because this is a rulemaking action.

(2) *Email: ISAO@lmi.org.* Include the docket number in the subject line of the message.

(3) *Mail:* ISAO Standards Organization, c/o LMI, 1777 NE Loop 410, Suite 808, San Antonio, TX 78217–5217.

To avoid duplication, please use only one of these three methods. All comments must either be submitted to the online docket on or before November 4, 2015, or reach the Docket Management Facility by that date.

Authority: 6 U.S.C. 131–134; 6 CFR 29; E.O.13691.

Dated: October 20, 2015.

Andy Ozment,

Assistant Secretary, Cybersecurity and Communications, National Protection and Programs Directorate, Department of Homeland Security.

[FR Doc. 2015–27102 Filed 10–23–15; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Intent To Request Renewal From OMB of One Current Public Collection of Information: Office of Law Enforcement/Federal Air Marshal Service Mental Health Certification

AGENCY: Transportation Security Administration, DHS.

ACTION: 60-day notice.

SUMMARY: The Transportation Security Administration (TSA) invites public comment on one currently approved Information Collection Request (ICR), Office of Management and Budget (OMB) control number 1652–0043, abstracted below, that we will submit to OMB for renewal in compliance with the Paperwork Reduction Act. The ICR describes the nature of the information collection and its expected burden. The collection involves a certification form that applicants for the Office of Law Enforcement/Federal Air Marshal Service are required to complete regarding their mental health history.

DATES: Send your comments by December 28, 2015.

ADDRESSES: Comments may be emailed to *TSAPRA@dhs.gov* or delivered to the TSA PRA Officer, Office of Information Technology (OIT), TSA–11, Transportation Security Administration, 601 South 12th Street, Arlington, VA 20598–6011.

FOR FURTHER INFORMATION CONTACT: Christina A. Walsh at the above address, or by telephone (571) 227–2062.

SUPPLEMENTARY INFORMATION:

Comments Invited

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*), an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The ICR documentation is available at *http://www.reginfo.gov.* Therefore, in preparation for OMB review and approval of the following information collection, TSA is soliciting comments to—

(1) Evaluate whether the proposed information requirement 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;

(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 using appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Information Collection Requirement

Pursuant to 49 U.S.C. 44917, TSA has authority to provide for deployment of Federal Air Marshals (FAMs) on passenger flights and provide for appropriate training, equipping, and supervision of FAMs. In furtherance of this authority, TSA policy requires that applicants for the Office of Law Enforcement/Federal Air Marshal Service positions meet certain medical and mental health standards.

In order to evaluate whether applicants meet TSA standards, applicants must undergo a psychological evaluation determining that they do not have an established medical history or clinical diagnosis of psychosis, neurosis, or any other personality or mental disorder that clearly demonstrates a potential hazard to the performance of FAM duties or the safety of self or others. As part of the psychological evaluation, applicants are required to complete a certification form regarding their mental health history and provide an explanation for anything they cannot certify. Applicants will be asked whether they can certify various statements including that they have never been removed from work for medical or psychological reasons.

Upon completion, applicants submit the certification form directly to the FAMS' Medical Programs Section (FAMS MPS) for initial screening via fax, electronic upload via scanning document, mail, or in person. The FAMS MPS screens all certification forms received. Any explanations for uncertified items received will generally require further review and follow-up by a personal psychologist or psychiatrist. This certification is carefully geared to capitalize on other elements of the assessment process, such as personal interviews, physical task assessment, background investigation, as well as the other components of the medical