

**DEPARTMENT OF HOMELAND SECURITY****Federal Emergency Management Agency**

[Internal Agency Docket No. FEMA-4764-DR]

[Docket ID FEMA-2024-0001]

**Maine; Amendment No. 1 to Notice of a Major Disaster Declaration****AGENCY:** Federal Emergency Management Agency, DHS.**ACTION:** Notice.**SUMMARY:** This notice amends the notice of a major disaster declaration for the State of Maine (FEMA-4764-DR), dated March 20, 2024, and related determinations.**DATES:** This change occurred on September 17, 2024.**FOR FURTHER INFORMATION CONTACT:** Dean Webster, Office of Response and Recovery, Federal Emergency Management Agency, 500 C Street SW, Washington, DC 20472, (202) 646-2833.**SUPPLEMENTARY INFORMATION:** The Federal Emergency Management Agency (FEMA) hereby gives notice that pursuant to the authority vested in the Administrator, under Executive Order 12148, as amended, Georgeta Dragoiu, of FEMA is appointed to act as the Federal Coordinating Officer for this disaster.

This action terminates the appointment of Robert V. Fogel as Federal Coordinating Officer for this disaster.

The following Catalog of Federal Domestic Assistance Numbers (CFDA) are to be used for reporting and drawing funds: 97.030, Community Disaster Loans; 97.031, Cora Brown Fund; 97.032, Crisis Counseling; 97.033, Disaster Legal Services; 97.034, Disaster Unemployment Assistance (DUA); 97.046, Fire Management Assistance Grant; 97.048, Disaster Housing Assistance to Individuals and Households In Presidentially Declared Disaster Areas; 97.049, Presidentially Declared Disaster Assistance—Disaster Housing Operations for Individuals and Households; 97.050, Presidentially Declared Disaster Assistance to Individuals and Households—Other Needs; 97.036, Disaster Grants—Public Assistance (Presidentially Declared Disasters); 97.039, Hazard Mitigation Grant.

**Deanne Criswell,***Administrator, Federal Emergency Management Agency.*

[FR Doc. 2024-24891 Filed 10-24-24; 8:45 am]

**BILLING CODE 9111-23-P****DEPARTMENT OF HOMELAND SECURITY**

[Docket No. CISA-2024-0024]

**National Security Telecommunications Advisory Committee****AGENCY:** Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).**ACTION:** Notice of partially closed Federal Advisory Committee meeting.**SUMMARY:** CISA is publishing this notice to announce the President's National Security Telecommunications Advisory Committee (NSTAC) Meeting on November 14, 2024, in Washington DC. This meeting will be partially closed to the public. The public can access the open portion of the meeting via teleconference.**DATES: Meeting Registration:** Registration to attend the meeting is required and must be received no later than 5 p.m. Eastern Standard Time (EST) on November 12, 2024. For more information on how to participate, please contact [NSTAC@cisa.dhs.gov](mailto:NSTAC@cisa.dhs.gov).**Speaker Registration:** Registration to speak during the meeting's public comment period must be received no later than 5 p.m. EST on November 7, 2024.**Written Comments:** Written comments must be received no later than 5 p.m. EST on November 7, 2024.**Meeting Date:** The NSTAC will meet on November 14, 2024, from 1 p.m. to 4:30 p.m. EST. The meeting may end early if the committee has completed its business.**ADDRESSES:** The NSTAC meeting will be open to the public, per 41 CFR 102-3.150 and will be held virtually. Members of the public may participate via teleconference only. For access to the conference call bridge, or to request special assistance, please email [NSTAC@mail.cisa.dhs.gov](mailto:NSTAC@mail.cisa.dhs.gov) by 5:00 p.m. EST on November 12, 2024. The NSTAC is committed to ensuring all participants have equal access regardless of disability status. If you require a reasonable accommodation due to a disability to fully participate, please contact the individual listed in the **FOR FURTHER INFORMATION CONTACT** section as soon as possible.**Comments:** Members of the public are invited to provide comments on issues that will be considered by the committee as listed in the **SUPPLEMENTARY INFORMATION** section below. Associated materials that may be discussed during the meeting will be made available for review at <https://>[www.cisa.gov/nstac](http://www.cisa.gov/nstac) prior to the day of the meeting. Comments should be submitted by 5:00 p.m. EST on November 7, 2024, and must be identified by Docket Number CISA-2024-0024. Comments may be submitted by one of the following methods:

- **Federal eRulemaking Portal:** [www.regulations.gov](http://www.regulations.gov). Please follow the instructions for submitting written comments.

- **Email:** [NSTAC@mail.cisa.dhs.gov](mailto:NSTAC@mail.cisa.dhs.gov). Include the Docket Number CISA-2024-0024 in the subject line of the email.

**Instructions:** All submissions received must include the words "Cybersecurity and Infrastructure Security Agency" and the Docket Number for this action. Comments received will be posted without alteration to[www.regulations.gov](http://www.regulations.gov), including any personal information provided. You may wish to review the Privacy & Security Notice available via a link on the homepage of [www.regulations.gov](http://www.regulations.gov).**Docket:** For access to the docket and comments received by the NSTAC, please go to [www.regulations.gov](http://www.regulations.gov) and enter docket number CISA-2024-0024.A public comment period is scheduled to be held during the meeting from 3:40 to 3:50 p.m. EST. Speakers who wish to participate in the public comment period must email [NSTAC@mail.cisa.dhs.gov](mailto:NSTAC@mail.cisa.dhs.gov) to register. Speakers should 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:** Christina Berger, 202- 701-6354, [NSTAC@mail.cisa.dhs.gov](mailto:NSTAC@mail.cisa.dhs.gov).**SUPPLEMENTARY INFORMATION:** The NSTAC is established under the authority of Executive Order (E.O.) 12382, dated September 13, 1982, as amended by E.O. 13286 and 14048, continued under the authority of E.O. 14109, dated September 30, 2023. Notice of this meeting is given under the Federal Advisory Committee Act (FACA), 5 U.S.C. Chapter 10. The NSTAC advises the President on matters related to national security and emergency preparedness (NS/EP) telecommunications and cybersecurity policy.**Agenda:** The NSTAC will meet in an open session on Thursday, November 14, 2024, from 3 p.m. to 4:30 p.m. EST to discuss current NSTAC activities and the government's ongoing cybersecurity and NS/EP communications initiatives. This open session will include: (1) an update on the administration's

cybersecurity initiatives; (2) a status update on the NSTAC Principles for Baseline Security Offerings from Cloud Service Providers Study; and (3) a status update on the National Preparedness for Post-Quantum Cryptography Study.

The committee will also meet in a closed session from 1:00 to 2:45 p.m. EST during which time: (1) senior government intelligence officials will provide a threat briefing concerning threats to NS/EP communications; and (2) NSTAC members and government officials will discuss potential future NSTAC study topics.

*Basis for Closure:* In accordance with section 1009(d) of FACA; and sections 552b(c)(1) and 552b(c)(9)(B) of *The Government in the Sunshine Act* (Sunshine Act), 5 U.S.C. 552b; it has been determined that a portion of the agenda requires closure.

*These agenda items are the:* (1) classified threat briefing, which will provide NSTAC members the opportunity to discuss information concerning threats to NS/EP communications with senior government intelligence officials; and (2) potential future NSTAC study topic discussion. The threat briefing will be classified at the top secret/sensitive compartmented information level. Disclosure of these threats during the briefing, as well as vulnerabilities and mitigation techniques, is a risk to the Nation's cybersecurity posture because adversaries could use this information to compromise commercial and government networks. Subjects addressed during the discussion are tentative and are under further consideration by the committee.

Therefore, this portion of the meeting has been closed pursuant to section 1009(d) of FACA, and sections 552b(c)(1) and 552b(c)(9)(B) of the Sunshine Act, because it will disclose matters that are classified and be likely to significantly frustrate implementation of one or more proposed agency actions.

Dated: October 18, 2024

**Christina Berger,**

*Designated Federal Officer, National Security Telecommunications Advisory Committee, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.*  
[FR Doc. 2024-24863 Filed 10-24-24; 8:45 am]

**BILLING CODE 9111-LF-P**

## DEPARTMENT OF HOMELAND SECURITY

### Transportation Security Administration

#### Intent To Request Revision From OMB of One Current Public Collection of Information: Security Appointment Center Visitor Request Form and Foreign National Vetting Request

**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 1652-0068, abstracted below, that we will submit to OMB for a revision in compliance with the Paperwork Reduction Act (PRA). The ICR describes the nature of the information collection and its expected burden. The collection involves gathering information from individuals who plan to visit all TSA facilities in the National Capital Region (NCR).

**DATES:** Send your comments by December 24, 2024.

**ADDRESSES:** Comments may be emailed to [TSAPRA@tsa.dhs.gov](mailto:TSAPRA@tsa.dhs.gov) or delivered to the TSA PRA Officer, Information Technology (IT), TSA-11, Transportation Security Administration, 6595 Springfield Center Dr., Springfield, 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 will be available at <https://www.reginfo.gov> upon its submission to OMB. 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

*OMB Control Number 1652-0068; Security Appointment Center (SAC) Visitor Request Form and Foreign National Vetting Request.* The Secretary of the Department of Homeland Security (DHS) is required to protect property owned, occupied, or secured by the Federal Government. *See* 40 U.S.C. 1315; *see also* 41 CFR 102-81.15 (requires Executive agencies to be responsible for maintaining security at their own or leased facilities). To implement this requirement, DHS policy requires all visitors to DHS facilities in the NCR<sup>1</sup> to have a criminal history records check through the National Crime Information Center system before accessing the facility.

TSA has established a visitor management process that meets DHS requirements. This process allows TSA to conduct business with visitors, including other Federal employees and contract employees, while managing risks posed by individuals entering the building who have not been subject to a full employee security background check. Once an individual's access is approved, TSA's Visitor Management System generates temporary badges that visitors must wear when entering TSA facilities in the NCR. This badge must be clearly visible for the duration of the individual's visit.

Visitors seeking to enter TSA facilities must also have a TSA-Federal employee as their host, and the host must complete the electronic TSA Form 2802, *Security Appointment Center (SAC) Visitor Request Form*. TSA Form 2802 requires that the Federal host employee provide the visitor's first and last name, date of birth, date and time of visit, visitor type (e.g., DHS or other government visitor, non-government individual), and whether the visitor is a foreign national visitor.<sup>2</sup> Although TSA requests the visitor to provide their social security number (SSN), the visitor is not required to provide this information. When provided, TSA uses the SSN to expedite vetting and to

<sup>1</sup> TSA facilities in the NCR include TSA Headquarters, the Freedom Center, the Transportation Security Integration Facility, and the Annapolis Junction facility.

<sup>2</sup> A person who is not a citizen of the United States.