November 13, 2020. Please note that the public comment period may end before the time indicated, following the last call for comments.

FOR FURTHER INFORMATION CONTACT: Jasper Cooke, Designated Federal Officer, Office of the National Advisory Council, Federal Emergency Management Agency, 500 C Street SW, Washington, DC 20472–3184, telephone (202) 646–2700, and email *FEMA-NAC@fema.dhs.gov.* The NAC website is *http://www.fema.gov/national-advisory-council.*

SUPPLEMENTARY INFORMATION: Notice of this meeting is given under the Federal Advisory Committee Act, 5 U.S.C. Appendix.

The NAC advises the FEMA Administrator on all aspects of emergency management. The NAC incorporates input from state, local, territorial and tribal governments, and the private sector in the development and revision of FEMA plans and strategies. The NAC includes a cross-section of officials, emergency managers, and emergency response providers from State, local, territorial and Tribal governments, the private sector, and nongovernmental organizations.

Agenda: On Tuesday, November 17, 2020, the NAC will discuss final recommendations, and vote on the recommendations and the report.

On Wednesday, November 18, 2020, the NAC will present recommendations to and receive feedback from leadership and discuss strategic priorities with FEMA leadership and topical experts.

The full agenda and any related documents for this meeting will be available by Friday, November 13, 2020, by contacting the person listed in **FOR FURTHER INFORMATION CONTACT** above.

Pete Gaynor,

Administrator, Federal Emergency Management Agency.

[FR Doc. 2020–23956 Filed 10–26–20; 11:15 am]

BILLING CODE 9111–48–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2020–0015]

Notice of President's National Security Telecommunications Advisory Committee Meeting

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

ACTION: Notice of meeting; request for comments.

SUMMARY: CISA is publishing this notice to announce the following President's National Security Telecommunications Advisory Committee (NSTAC) meeting. This meeting will be partially closed to the public.

DATES:

Meeting Registration: Registration to attend the meeting is required and must be received no later than 5:00 p.m. Eastern Time (ET) on November 5, 2020. For more information on how to participate, please contact *NSTAC@cisa.dhs.gov.*

Speaker Registration: Registration to speak during the meeting's public comment period must be received no later than 5:00 p.m. ET on November 5, 2020.

Written Comments: Written comments must be received no later than 5:00 p.m. ET on November 5, 2020.

Meeting Date: The NSTAC will meet on November 12, 2020, from 12:30 p.m. to 4:15 p.m. ET. The meeting may close early if the committee has completed its business.

ADDRESSES: The meeting will be held via conference call. For access to the conference call bridge, information on services for individuals with disabilities, or to request special assistance, please email *NSTAC@cisa.dhs.gov* by 5:00 p.m. ET on November 5, 2020.

Comments: 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 materials that participants may discuss during the meeting will be available at *https://www.cisa.gov/national-security-telecommunications-advisory-committee* for review on October 28, 2020. Comments may be submitted by 5:00 p.m. ET on November 5, 2020 and must be identified by Docket Number CISA–2020–0015. Comments may be submitted by one of the following methods:

- *Federal eRulemaking Portal: www.regulations.gov.* Please follow the instructions for submitting written comments.
- *Email: NSTAC@cisa.dhs.gov.* Include the Docket Number CISA–2020–0015 in the subject line of the email.

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 to *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 CISA–2020–0015.

A public comment period will be held during the meeting from 3:15 p.m. to 3:25 p.m. ET. Speakers who wish to participate in the public comment period must register by emailing *NSTAC@cisa.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: Sandra Benevides, 703–705–6232, *sandra.benevides@cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION: The NSTAC was established by Executive Order (E.O.) 12382, 47 FR 40531 (September 13, 1982), as amended and continued under the authority of E.O. 13889, dated September 27, 2019. Notice of this meeting is given under FACA, 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 NSTAC will hold a conference call on Thursday, November 12, 2020, to discuss current NSTAC activities pertinent to Government cybersecurity initiatives and NS/EP priorities with senior Government officials. This meeting will include an open and closed session. During the open session, NSTAC members will: (1) Participate in a strategic discussion on promoting U.S. leadership in emerging information and communications technologies (ICT); (2) receive a status update from the NSTAC Communications Resiliency Subcommittee; and (3) receive a keynote address.

Basis for Closure: In accordance with section 10(d) of FACA and *The Government in the Sunshine Act* (5 U.S.C. 552b(c)(9)(B)), it has been determined that certain agenda items require closure, as the disclosure of the information that will be discussed would not be in the public interest.

The committee will meet in a closed session from 12:30 p.m. to 2:00 p.m. Participants will engage in discussions on key NS/EP communications topics, which may include strategic considerations for hardware and chipsets. The NSTAC will also discuss potential study topics for the upcoming work cycle. For these items, Government officials will share data with NSTAC members on ongoing NS/EP, cybersecurity, and communications resiliency initiatives across the public

and private sectors. The information discussed will include specific vulnerabilities that affect the United States' national defense/homeland security posture and ICT risk mitigation strategies. The premature disclosure of this information to the public is likely to frustrate implementation of proposed Government action significantly. Therefore, this portion of the meeting is required to be closed pursuant to section 10(d) of FACA and *The Government in the Sunshine Act* (5 U.S.C. 552b(c)(9)(B)).

Sandra J. Benevides,

Designated Federal Officer, NSTAC, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

[FR Doc. 2020–23835 Filed 10–27–20; 8:45 am]

BILLING CODE 9910–9P–P

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

[Docket No. TSA–2003–14610]

Notice To Extend Exemption From Renewal of the Hazardous Materials Endorsement Security Threat Assessment for Certain Individuals

AGENCY: Transportation Security Administration, DHS.

ACTION: Notice, extension of temporary exemption.

SUMMARY: TSA is extending the exemption from Renewal of the Hazardous Materials Endorsement Security Threat Assessment for Certain Individuals that TSA published on July 31, 2020 which was scheduled to expire on October 30, 2020, through December 31, 2020. Under this exemption, states may extend the expiration date of hazardous materials endorsements (HMEs) that expire on or after March 1, 2020, for 180 days, due to restrictions and business closures in place in response to the COVID–19 pandemic. If a state grants an extension, the individual with an expired HME must initiate the process of renewing his or her security threat assessment (STA) for the HME no later than 60 days before the end of the state-granted extension. Federal partners, state licensing agencies and related associations report ongoing difficulties in timely renewal of expiring HMEs and asked TSA to consider extending the exemption until the end of calendar year 2020. TSA has determined it is in the public interest to extend the exemption through December 31, 2020, which aligns with similar waivers issued by the U.S. Department of Transportation. TSA may extend this exemption at a future date depending on the status of the COVID–19 crisis.

DATES: This extension of the previously issued exemption published on July 31, 2020 (85 FR 46152) becomes effective on October 30, 2020, and remains in effect through December 31, 2020, unless otherwise modified by TSA through a notice published in the **Federal Register**.

FOR FURTHER INFORMATION CONTACT: Stephanie Hamilton, 571–227–2851 or *HME.question@tsa.dhs.gov.*

SUPPLEMENTARY INFORMATION:

Background

A public health emergency exists in this country as a consequence of the COVID–19 pandemic.[1] In response to this pandemic, on April 2, 2020, TSA issued an exemption from requirements in 48 CFR part 1572 regarding expiration of a TSA security threat assessment (STA) for HMEs.[2] TSA subsequently extended the duration of the exemption through October 29, 2020.[3]

The USA PATRIOT Act of 2001 requires individuals who transport hazardous materials via commercial motor vehicle to undergo a STA conducted by TSA.[4] As required by TSA's implementing regulations in 49 CFR part 1572, the STA for an HME consists of criminal, immigration, and terrorist checks. The STA and HME remain valid for five years.

Under 49 CFR 1572.13(a), no state may issue or renew an HME for an individual's commercial driver's license (CDL), unless the state first receives a Determination of No Security Threat for the individual from TSA following the STA. An individual seeking renewal of an HME must initiate an STA at least 60 days before expiration of his or her current HME.[5] The process of initiating an STA requires the individual to submit information either to the state licensing agency or a TSA enrollment center, including fingerprints and the information required by 49 CFR 1572.9,[6] at least 60 days before the expiration of the HME.[7]

It may be impracticable for some commercial drivers to renew their STAs during the current COVID–19 crisis. Measures to prevent the spread of COVID–19 may affect the ability of commercial drivers to present themselves in-person to a state licensing agency or TSA enrollment center for the collection of fingerprints and applicant information. Without the new STA, TSA's regulations prevent states from renewing or extending the expiration of the individual's state-issued HME.[8]

Consistent with the requirements in 49 CFR 1572.13(b), if the state grants an extension to a driver, the state must, if practicable, notify the driver that the state is extending the expiration date of the HME, the date that the extension will end, and the individual's responsibility to initiate the STA renewal process at least 60 days before the end of the extension. If it is not practicable for a state to give individualized notice to drivers, the state may publish general notice, for example, on the appropriate website.

Authority and Determination

TSA may grant an exemption from a regulation if TSA determines that the exemption is in the public interest.[9] On April 2, 2020, TSA determined that it was in the public interest to grant an exemption from certain process requirements in 49 CFR part 1572 related to STAs for HMEs, given the need for HME drivers to work without interruption during the COVID–19 crisis.[10] On July 31, 2020, TSA extended that exemption by 90 days through October 29, 2020.[11] TSA has determined that it is in the public interest to extend the exemption through December 31, 2020.

The exemption does not compromise the current level of transportation security because TSA continues to conduct recurrent security threat checks on HME holders and is able to take action to revoke an HME if derogatory information becomes available, regardless of expiration date. TSA uses data previously submitted by these

[1] *See* HHS, Renewal of Determination that a Public Health Emergency Exists (Oct. 2, 2020), available at *https://www.phe.gov/emergency/news/healthactions/phe/Pages/covid19-2Oct2020.aspx. See also* Proclamation 9994, *Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID–19) Outbreak* (March 13, 2020). Published at 85 FR 15337 (Mar. 18, 2020).

[2] *See* 85 FR 19767 (April 8, 2020).

[3] *See* 85 FR 46152 (July 31, 2020).

[4] Public Law 107–56 (Oct. 26, 2001; 115 Stat. 396), § 1012(a)(1), *codified as amended at* 49 U.S.C. 5103a.

[5] 49 CFR 1572.13(b).

[6] 49 CFR 1572.15.

[7] 49 CFR 1572.13(b).

[8] 49 CFR 1572.13(a).

[9] 49 U.S.C. 114(q). The Administrator of TSA delegated this authority to the Executive Assistant Administrator for Operations Support, effective March 26, 2020, during the period of the National Emergency cited supra, n. 1.

[10] *See* Exemption from Renewal of the Hazardous Materials Endorsement Security Threat Assessment for Certain Individuals, 85 FR 19767 (Apr. 8, 2020).

[11] *See* Notice to Extend Exemption from Renewal of the Hazardous Materials Endorsement Security Threat Assessment for Certain Individuals, 85 FR 46152 (July 31, 2020).