Total Annualized Respondent Opportunity Cost: $16,215.

Total Annualized Respondent Out-of-Pocket Cost: $0.

Total Annualized Government Cost: $3,000,000.

Robert Costello,

Chief Information Officer, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency.

[FR Doc. 2022–23987 Filed 11–3–22; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2022–0050]

Homeland Security Advisory Council

AGENCY: The Department of Homeland Security (DHS), The Office of Partnership and Engagement (OPE).

ACTION: Notice of new taskings for the Homeland Security Advisory Council (HSAC).

SUMMARY: On October 16, 2022 the Secretary of DHS, Alejandro N. Mayorkas, tasked the Homeland Security Advisory Council (HSAC) to establish four new subcommittees further outlined below. This notice is not a solicitation for membership.

FOR FURTHER INFORMATION CONTACT: Rebecca Sternhell, Executive Director of the Homeland Security Advisory Council, Office of Partnership and Engagement, U.S. Department of Homeland Security at *HSAC@hq.dhs.gov* or 202–891–2876.

SUPPLEMENTARY INFORMATION: The HSAC provides organizationally independent, strategic, timely, specific, and actionable advice and recommendations for the consideration of the Secretary of the Department of Homeland Security on matters related to homeland security. The HSAC is comprised of leaders in local law enforcement, first responders, public health, State, local and tribal government, national policy, the private sector, and academia.

The four new subcommittees are as follows:

Subcommittee (1): DHS Leadership in Supply Chain Security

A subcommittee to provide recommendations on how the Department can take a greater leadership role in supply chain security, including by strengthening supply chain cybersecurity.

Subcommittee (2): DHS Intelligence and Information Sharing

A subcommittee to provide recommendations on how the Department can improve upon its intelligence and information sharing with our key federal, state, local, tribal, territorial, and private sector partners. The subcommittee will assess whether the Department's information sharing architecture developed by the DHS Office of Intelligence and Analysis (I&A) is adequate for the threats of today and tomorrow, and provide advice and recommendations to better enable the Office of Intelligence and Analysis (I&A) to rapidly and efficiently share information and intelligence with our key partners.

Subcommittee (3): DHS Transparency and Open Government

A subcommittee to provide recommendations on how the Department can improve its commitment to transparency and open government. The subcommittee will provide advice and recommendations that will position the Department as the leader in this critical area of model government conduct.

Subcommittee (4): Homeland Security Technology and Innovation Network

A subcommittee to provide recommendations on how the Department can create a more robust and efficient Homeland Security Technology and Innovation Network. The subcommittee will provide advice and recommendations that will develop the Department's innovation, research and development, and technology network with the private sector.

Tasking (1): DHS Leadership in Supply Chain Security

The United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security. DHS continues to protect America's national and economic security by facilitating legitimate trade and travel and rigorously enforcing U.S. customs and immigration laws and regulations.

As the Department strives to stay ahead of the curve and take a greater leadership role by harnessing new technologies, minimizing environmental impact, and increasing partnerships in this vital area, this HSAC subcommittee is tasked to provide recommendations on how the Department can take a greater leadership role in supply chain security. The subcommittee's assessment will include, but need not be limited to, the following:

a. strengthening physical security;

b. strengthening cybersecurity; and,

c. increasing efficiencies to ensure a resilient, safe, and secure supply chain for critical manufacturing and technology sectors.

Tasking (2): DHS Intelligence and Information Sharing

Federal, state, local, tribal, and territorial partners convened shortly after the September 11, 2001 terrorist attacks, creating a domestic information sharing architecture to enable the timely and seamless exchange of information to detect and eliminate terrorist threats. In the 21 years since 9/11, our law enforcement and homeland security community has made great progress in reshaping our information sharing environment. Working together, we put policies and processes in place that help us to be safer and more secure than we were years ago.

As the Department approaches its 20th Anniversary, the HSAC subcommittee is asked to provide recommendations on:

1. How the Department can rapidly and efficiently share intelligence and information with its federal, state, local, tribal, territorial, and private sector partners. Have DHS investments in information sharing technology and changes in law and policy resulted in increased knowledge transfer and resilience? Are further investments or changes in law or policy needed?

2. Has DHS created an information and intelligence sharing architecture that efficiently spreads knowledge and rapidly shares critical information? Are there steps that we need to take to revitalize or improve this architecture?

3. Whether the current DHS information sharing architecture optimizes information sharing for threats other than counterterrorism; for example, cyber, border security, foreign influence/propaganda, strategic advantage, and others.

4. Internal DHS Information Sharing: Has DHS fully implemented internal DHS information sharing policy—for example, the One DHS Memo—to leverage DHS data and information to support Departmental missions like border security as well as to develop and share relevant, quality intelligence with our partners?

Tasking (3): DHS Transparency and Open Government

DHS is committed to transparency and promoting the principles of an Open Government. The United States has worked both domestically and internationally to ensure global support for Open Government principles to promote transparency, fight corruption, energize civic engagement, and leverage new technologies in order to strengthen

the foundations of freedom in our own nation and abroad.

DHS has expanded transparency in concert with the development of Open Government Plans, recognizing that increased access to research data and information can encourage research collaboration and help successfully address the nation's constantly evolving homeland security challenges.

The HSAC subcommittee is asked to provide recommendations on:

1. How the Department and its components can expand on the foundation set by previous Open Government Plans for DHS.

2. New initiatives to increase transparency and sustaining the DHS mission to protect the homeland.

3. How DHS can be held accountable in meeting its commitment to be a leader in modeling government openness and transparency.

Tasking (4): Homeland Security Technology and Innovation Network

DHS employs more than 240,000 individuals working in multiple offices and components across the country and the world. While the mission is uniform across the Department—to protect the homeland from foreign and domestic threats—the tools necessary to accomplish this can vary widely by office and can change in time. Moreover, while some threats are known and have been core to the DHS mission since its inception, we must remain ever vigilant and responsive to countering both unknown and future threats. In this scenario we may face accelerated timelines that do not fit into our normal acquisition life cycle to acquire key technology to counter a threat. It is critical to our nation's security to have a robust and efficient Homeland Security Technology and Innovation Network that promotes an enhanced schedule of development and deployment of critical technology and assets to protect the homeland.

To maximize the opportunity afforded by partnership with the private sector and the expertise within the Department, the HSAC subcommittee is asked to assess the private sector experience, specifically in the areas of technology development and innovation, and provide recommendations on how the Department can create a more robust and efficient Homeland Security Technology and Innovation Network. The subcommittee's assessment will include, but need not be limited to, the following:

a. an assessment of how the private sector engages with the current Research and Development (R&D) and acquisition programs and opportunities, including where those can be maximized or improved;

b. different means of increasing innovative technology partnerships with the private sector;

c. recommendations on harmonizing existing innovation efforts across the Department and its components to best leverage funding and resources; and

d. identifying current barriers to developing a more robust technology and innovation network, including legal, contracting, and policy considerations.

Schedule: The four subcommittees' findings and recommendations will be submitted to the HSAC for its deliberation and vote during a public meeting. Once the recommendations from the four subcommittees are voted on by the HSAC, they will be submitted to the Secretary. The four subcommittees will submit their findings and recommendations to the HSAC in March 2023.

Dated: October 26, 2022.

Rebecca K.K. Sternhell,

Executive Director, Homeland Security Advisory Council, Department of Homeland Security.

[FR Doc. 2022–24042 Filed 11–3–22; 8:45 am]

BILLING CODE 9112–FN–P

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

[Docket No. TSA–2004–19605]

Hazardous Materials Endorsement (HME) Threat Assessment Program and Transportation Worker Identification Credential (TWIC®) Program Fees

AGENCY: Transportation Security Administration, DHS.

ACTION: Notice.

SUMMARY: The Transportation Security Administration (TSA) administers the Hazardous Materials Endorsement (HME) and Transportation Worker Identification Credential (TWIC®) vetting programs. TSA conducts security threat assessments (STAs) of applicants to these programs, and in accordance with statutory requirements, collects fees from the applicants to recover TSA's costs to conduct the vetting and credentialing. In this Notice, TSA announces changes to the existing fee structure and fees for the HME and TWIC Programs to include initial in-person applications, in-person renewals, comparable STAs, and new online renewal fees. These updates will allow TSA to continue to improve the HME and TWIC enrollment experience, mitigate potential security risks, and ensure that the programs remain fully funded. TSA maintains a current listing of the overall fees for all HME enrollment options at *https://www.tsa.gov/for-industry/hazmat-endorsement* and for all TWIC enrollment options at *https://www.tsa.gov/for-industry/twic.*

DATES: The fee changes in this notice are effective November 3, 2022.

FOR FURTHER INFORMATION CONTACT: Stephanie Hamilton, Transportation Security Administration, 6595 Springfield Center Drive, Springfield, VA 20598–6047; 571–227–2851; or email at *TWIC.Issue@tsa.dhs.gov* and *HME.Question@tsa.dhs.gov.*

SUPPLEMENTARY INFORMATION: You can find an electronic copy of rulemaking documents relevant to this action by searching the electronic FDMS web page at *https://www.regulations.gov* or at *https://www.federalregister.gov.* In addition, copies are available by writing or calling the individual in the **FOR FURTHER INFORMATION CONTACT** section.

Abbreviations and Terms Used in This Document

CDL—Commercial Driver's License
CHRC—Criminal History Records Check
FBI—Federal Bureau of Investigation
FAST—Free and Secure Trade
HME—Hazardous Materials Endorsement
MTSA—Maritime Transportation Security Act
STA—Security Threat Assessment
TWIC—Transportation Worker Identification Credential
UES—Universal Enrollment Services
USCG—U.S. Coast Guard

I. TWIC Program

A. Background

The Maritime Transportation Security Act (MTSA) of 2002 requires the Secretary of the Department of Homeland Security to issue a biometric transportation security card to an individual requiring unescorted access to MTSA-regulated entities after determining that the individual does not pose a security risk.[1] The TWIC Program is administered jointly by TSA and the U.S. Coast Guard (USCG). TSA conducts the STA and issues the credential, and USCG enforces the use of the TWIC at MTSA-regulated facilities and vessels.[2]

Under TSA's regulations in 49 CFR part 1572, applicants for TWIC pay a fee to cover (1) the costs of performing and

[1] *See* Maritime Transportation Security Act of 2002, Public Law 107–295, 116 Stat. 2064 (November 25, 2002).

[2] *See* 46 U.S.C. 70105.