on cyber threat indicators, defense measures, cybersecurity risks, incidents, analyses, and warnings to help small business concerns in developing or enhancing cybersecurity infrastructure, awareness of cyber threat indicators, and cyber training programs for employees.'' 6 U.S.C. 148(l); see also 15 U.S.C. 648(g) (similarly authorizing DHS, ''and any other Federal department or agency in coordination with the Department of Homeland Security'' to ''leverage small business concerns by disseminating information relating to cybersecurity risks and other homeland security matters to help small business concerns in developing or enhancing cybersecurity infrastructure, awareness of cyber threat indicators, and cyber training programs for employees'').

Consistent with these authorities, E.O. 13636 directs the Department to increase its cybersecurity information sharing efforts with the private sector and consult on and promote the National Institute of Standards and Technology (NIST) Cybersecurity Framework. To facilitate the Department's promotion of the NIST Cybersecurity Framework, the E.O. directs the Secretary to establish a voluntary program to support the adoption of the Framework in coordination with Sector Specific Agencies, which in turn ''shall coordinate with Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.'' E.O. No. 13636, 78 FR 11739 (2013).

Accordingly, the Information Technology (IT) Sector, represented by industry via the IT Sector Coordinating Council (SCC) and by Government via the IT Government Coordinating Council (GCC), established the IT Sector Small and Midsized Business (SMB) Cybersecurity Best Practices Working Group (''Working Group'') to develop best practices for implementing the NIST Cybersecurity Framework in the SMB community. The Working Group, which consists of industry and government representatives, developed the SMB Cybersecurity Survey to determine Return on Investment (ROI) metrics for NIST Cybersecurity Framework adoption among SMB stakeholders. This process will assess the effectiveness of the NIST Cybersecurity Framework. This process will also establish a baseline for ROI metrics, which have not previously existed in the SMB community. The IT Sector-Specific Agency (SSA),

headquartered in DHS CS&C, is supporting the Working Group's survey development.

DHS is not administering, controlling or soliciting the collection of the information via the survey. The IT SCC will administer the survey and anonymize the data, which will then be sent to DHS for analysis. DHS is not administering or soliciting the collection of information via the survey. The analysis will determine ROI information for NIST Cybersecurity Framework adoption in the SMB community. The results of this analysis will be used to provide the SMB community with best practices on how to use the Cybersecurity Framework for business protection and risk management.

The questionnaire will be distributed to SMBs and is a two-part survey. Questions 1–11 of the survey are for an organization's leadership, as these questions pertain to high level information about the company (core function, number of employees, etc.). The remaining questions are intended for the Chief Information Services Officer (CISO) and/or appropriate IT staff, as these questions are technical and ask about the IT security of the company.

The private sector will collect Point of Contact (POC) information through the survey instrument, but will not include that information on the anonymized dataset they submit to DHS. DHS will use anonymized data to conduct their analysis. The IT SCC will administer the survey.

The intent is for DHS to only receive derivative products—anonymized micro-dataset to come up with the summary statistics, or aggregated summary results. The IT SCC will conduct the actual data collection. DHS will aid with the statistical analysis where needed, but would not be working with the individual responses to the questionnaire. Even if the POC question does get included in the questionnaire, DHS would not be collecting or retaining PII.

Once the survey is administered by the private sector partners of the IT SCC to the member organizations, the collected raw inputs will be compiled and the resulting dataset will be processed by the private sector partners to (a) assign unique random identifiers to each of the responses, (b) scrub any PII from the microdata, (c) QA against the raw input. These processing steps (a–c) will be implemented PRIOR to handing the dataset to DHS for statistical analysis. This survey represents a new collection.

OMB is particularly interested in comments that:

1. Evaluate whether the proposed collection of information 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 of the proposed collection of information, including the validity of the methodology and assumptions used;

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 through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.,* permitting electronic submissions of responses.

Analysis

Agency: Department of Homeland Security, National Protection and Programs Directorate, Office of Cybersecurity and Communications, Stakeholder Engagement & Cyber Infrastructure Resilience Division.

Title: The Department of Homeland Security, Stakeholder Engagement & Cyber Infrastructure Resilience Division.

OMB Number: 1670—NEW.

Frequency: Once every five years.

Affected Public: Private sector, Small & Midsize Business (SMB).

Number of Respondents: 1,000 annually.

Estimated Time per Respondent: 30 minutes.

Total Burden Hours: 500 annual burden hours.

Total Burden Cost (capital/startup): $0.

Total Recordkeeping Burden: $0.

Total Burden Cost (operating/ maintaining): $0.

Dated: July 12, 2017.

David Epperson,

Chief Information Officer.

[FR Doc. 2017–15068 Filed 7–17–17; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Intent To Request Approval From OMB of One New Public Collection of Information: Military Severely Injured Joint Support Operations Center (MSIJSOC) and Travel Protocol Office (TPO) Programs

AGENCY: Transportation Security Administration, DHS.

ACTION: 60-Day notice.

SUMMARY: The Transportation Security Administration (TSA) invites public comment on a new Information Collection Request (ICR) abstracted below, that we will submit to the Office of Management and Budget (OMB) for approval in compliance with the Paperwork Reduction Act (PRA). The ICR describes the nature of the information collection and its expected burden. The collection involves the submission of travel information to TSA to provide wounded warriors, severely injured military personnel, and certain other travelers with assistance through the airport security screening process.

DATES: Send your comments by September 18, 2017.

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 will be made available at *http://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

Purpose and Description of Data Collection

The Transportation Security Administration (TSA) established the Military Severely Injured Joint Support Operations Center (MSIJSOC) and the Travel Protocol Office (TPO) programs to support and facilitate the movement of wounded warriors, severely injured military personnel, veterans and other travelers requiring an escort through the airport security screening process. The MSIJSOC and TPO programs are available at commercial airports within the continental United States and its territories.

The MSIJSOC program works with passengers who are wounded warriors, severely injured military members, and veterans. Once flight arrangements are made with the airlines, the traveler, his or her family, or other representative may contact the TSA Cares Hotline no later than 72 hours prior to their scheduled flight time with the details of the itinerary. TSA will collect the traveler's name, travel itinerary (flight departure and arrival information), and a point-of-contact's mobile phone number. Once TSA collects this information, TSA Cares will contact MSIJSOC, where the staff will vet the request via the appropriate Wounded Warrior Care Coordinator to verify the wounded warriors, severely injured military members, and veterans' eligibility. After verifying eligibility, the MSIJSOC will contact the respective TSA official at the appropriate airport for action.

Additionally, the TPO program facilitates the movement of foreign dignitaries, accredited Ambassadors to the United States and others who may require an escort through the airport security screening process. These travelers may contact the TPO office by submitting a request for travel support via telephone. Travelers and their points-of-contact should submit their travel support requests no later than 72 hours prior to the respective scheduled flight to allow TSA to make timely notification regarding the travel. TSA will collect the traveler's name, travel itinerary (flight departure and arrival information), and a point-of-contact's mobile phone number.

The estimated annual burden for this collection is 467 hours. The estimated number of annual respondents is 5,600 with each response taking approximately 0.0833 hours (5600 × 0.0833).

Dated: July 12, 2017.

Christina A. Walsh,

TSA Paperwork Reduction Act Officer, Office of Information Technology.

[FR Doc. 2017–15019 Filed 7–17–17; 8:45 am]

BILLING CODE 9110–05–P

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

[FWS–R2–ES–2016–0141; FXES11140200000–178–FF02ENEH00]

Draft Environmental Impact Statement and Draft Barton Springs Edwards Aquifer Conservation District Habitat Conservation Plan

AGENCY: Fish and Wildlife Service, Interior.

ACTION: Notice of availability: notice of receipt of a permit application; and announcement of a public meeting.

SUMMARY: We, the U.S. Fish and Wildlife Service (Service), announce the availability of a draft environmental impact statement (dEIS), which evaluates the impacts of, and alternatives to, the proposed Barton Springs Edwards Aquifer Conservation District (BSEACD) Habitat Conservation Plan (dHCP) for federally-listed Barton Springs salamander (BSS) and Austin blind salamander (ABS) (collectively, covered species) incidental take in portions of Travis and Hays Counties, Texas, where pumping withdrawals are implemented, authorized, or permitted by BSEACD. We also announce that we will hold a public meeting on this project.

DATES: *Comments:* We will accept comments received or postmarked on or before September 18, 2017. Comments submitted electronically using the Federal eRulemaking Portal (see **ADDRESSES** section below) must be received by 11:59 p.m. Eastern Time on the closing date. Any comments that we receive after the closing date may not be considered in the final decision on these actions.

ADDRESSES: *Obtaining Documents:*

• *Internet:* You may obtain copies of the dEIS and dHCP on the Federal eRulemaking Portal at *http://www.regulations.gov* (Docket Number FWS–R2–ES–2016–0141); or

• You may also obtain copies of the dEIS and dHCP on the Service's Web site at *http://www.fws.gov/southwest/es/AustinTexas/* (refer to permit number TE10607C).

• *U.S. Mail:* A limited number of CD–ROM and printed copies of the dEIS and dHCP are available, by request, from the Field Supervisor, U.S. Fish and Wildlife Service, 10711 Burnet Road, Suite 200, Austin, TX 78758; phone (512) 490–0057; or fax (512) 490–0974. Please note that your request is in reference to the HCP for BSS and ABS (TE10607C).

• *In-Person:* Copies of the dEIS and dHCP are also available for public