9110-9P P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2017-0034]

Information Collection Request: The Department of Homeland Security, Stakeholder Engagement and Cyber Infrastructure Resilience Division(SECIR)

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: 60-day notice and request for comments.

SUMMARY: The Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), Office of Cybersecurity and Communications (CS&C), Stakeholder Engagement & Cyber Infrastructure Resilience Division (SECIR), will submit the following Information Collection Request to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995.

DATES: Comments are encouraged and will be accepted until ***[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].*** This process is conducted in accordance with 5 CFR 1320.1.

ADDRESS: Written comments and questions about this Information Collection Request should be forwarded to DHS/NPPD/CS&C/SECIR, 4200 Wilson Blvd, Mail Stop 0412, Arlington,VA 22203-0412. E-mailed requests should go to

nppd-prac@HQ.DHS.GOV. Written comments should reach the contact person listed no later than ***[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].*** Comments must be identified by "DHS-2017-0034"and may be submitted by one of the following methods:

- **Federal eRulemaking Portal:** http://www.regulations.gov. Follow the instructions for submitting written comments.
- **E-mail:** nppd-prac@HQ.DHS.GOV. Please include the docket number DHS-2017-0034 in the subject line of the message.

  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 at http://www.regulations.gov.

SUPPLEMENTARY INFORMATION: Section 227 of the Homeland Security Act authorizes the National Cybersecurity and Communications Integration Center (NCCIC) within NPPD as a "Federal civilian interface for the multi-directional and cross-sector sharing of information related to . . . cybersecurity risks." 6 U.S.C. 148(c)(1). This authority applies to Federal and non-Federal entities, including the private sector, small and medium businesses, sectors of critical infrastructure, and information sharing organizations. This provision includes the authority to receive, analyze and disseminate information about

cybersecurity risks and incidents and to provide guidance, assessments, incident response support, and other technical assistance upon request and codifies NPPD's coordinating role among federal and non-federal entities. 6 U.S.C. 148.

As part of its information sharing responsibilities with non-Federal entities, the National Defense Authorization Act For Fiscal Year 2017 amended the Homeland Security Act to authorize the Department to specifically focus on small businesses. See Pub. L. No. 114-328 (2017). Specifically, the Act authorizes NPPD to "leverage small business development centers to provide assistance to small business concerns by disseminating information 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: 7/17/2017 8:45 am; Publication Date: 7/18/2017]