9110-9P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA-2023-0019]

Agency Information Collection Activities: ReadySetCyber Initiative Questionnaire

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

ACTION: 60-day notice and request for comments on a new collection

SUMMARY: CISA will submit the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and clearance.

DATES: Comments are encouraged and will be accepted until ***[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].***

ADDRESSES: You may submit comments, identified by docket number Docket # CISA-2023-0019, at:

- Federal eRulemaking Portal: http://www.regulations.gov. Please follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name and docket number Docket # CISA- 2023-0019. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

SUPPLEMENTARY INFORMATION: Consistent with CISA's authorities to "carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States" at 6 U.S.C. 652(e)(1)(B) and provide federal and non-federal entities with "operational and timely technical assistance" at 6 U.S.C. 659(c)(6) and "recommendation on security and resilience measures" at 6 U.S.C. 659(c)(7), CISA's ReadySetCyber Initiative will collect information in order to provide tailored technical

assistance, services and resources to critical infrastructure (CI) organizations and state, local, tribal, and territorial (SLTT) governments based on the characteristics of their respective cybersecurity programs. CISA seeks to collect this information from US CI and SLTT organizations on a voluntary and fully electronic basis so that each organization can be best supported in receiving tailored cybersecurity recommendations and services.

The overarching goal of CISA's ReadySetCyber Initiative is to help CI and SLTT organizations access information and services that are tailored to their specific cybersecurity needs. In addition, CISA expects this initiative to yield several additional benefits, including:

- Further adoption of CISA's Cybersecurity Performance Goals (CPGs) as the default approach for assessing Organizational progress and identify prioritized cybersecurity gaps;
- Collection of information about organizations' cybersecurity posture and progress, enabling more targeted engagement with sectors, regions, and individual organizations;
- More effective allocation of capacity-constrained services to specific stakeholders;
- Provision of a simplified approach to the guiding stakeholders into enrollment for, scalable services and rapidly expand uptake thereof; and
- Furthering the development of relationships between CI and SLTT organizations and CISA's regional cybersecurity personnel.

CISA's CPGs are a set of voluntary cybersecurity practices which aim to reduce the risk of cybersecurity threats to U.S. CI and SLTT organizations. CISA offers services and resources to aid CI and SLTT organizations in adopting the CPGs and seeks to make

accessing appropriate services and resources as efficient as possible, especially for organizations whose cybersecurity programs operate at low levels of capability.

For example, an organization that is unsure of its ability to enumerate all of its internet-facing sites and services could leverage CISA's highly scalable automated testing services to scan its entire network range. Organizations with cybersecurity programs with more advanced characteristics who wish to evaluate their network segmentation controls are better positioned to take advantage of CISA's more resource-intensive architecture assessments. All organizations completing the questionnaire will also be connected with a CISA cybersecurity representative in their jurisdiction to provide direct support and engagement.

To measure adoption of the CPGs and assist CI and SLTT organizations in finding the most impactful services and resources for their cybersecurity programs, CISA is seeking to establish a voluntary information collection that uses respondents' answers to tailor a recommended package of services and resources most applicable to their evaluated level of program capability. Without collecting this information, CISA would be unable to tailor an appropriate suite of services, recommendations, and resources to assist the organization in protecting itself against cybersecurity threats, thereby creating burdens of inefficiency for service requesters and CISA alike.

In addition, receipt of this information is critical to CISA's ability to measure the adoption of CISA's CPGs by CI and SLTT organizations. The information to be collected will address various inquiries, such as: whether an organization keeps a regularly updated inventory of all assets with an Internet Protocol address; the types of incident reporting and vulnerability disclosures required by an organizations' contracts with its vendors and suppliers; and whether the entity requires a minimum password strength required for all password-protected assets.

The Office of Management and Budget is particularly interested in comments which:

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

Title: ReadySetCyber

OMB Number:

Frequency: Upon each voluntary request for technical assistance, which CISA expects to occur on an annual basis.

Affected Public: Critical Infrastructure Owners & Operators seeking CISA services

Number of Respondents: Approximately 2,000 per year

Estimated Time Per Respondent: 20 Minutes

Total Burden Hours: 666.7 Hours

Robert J. Costello,

Chief Information Officer,
Department of Homeland Security,
Cybersecurity and Infrastructure Security Agency.
[FR Doc. 2023-17183 Filed: 8/9/2023 8:45 am; Publication Date: 8/10/2023]