



9110-9P P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2017-0032]

New Information Collection Request: The Department of Homeland Security, Office of Cybersecurity and Communications, US-CERT.gov Collection

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), National Cybersecurity and Communications Integration Center (NCCIC), United States Computer Emergency Readiness Team (US-CERT) 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.

ADDRESSES: Written comments and questions about this Information Collection Request should be forwarded to DHS/NPPD/CS&C/NCCIC/US-CERT, 245 Murray Lane, SW, Mail Stop

0640, Arlington, VA 20598-0640. E-mailed requests should go to info@us-cert.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-2017-0032" and may be submitted by one of the following methods:

- **Federal eRulemaking Portal:** <http://www.regulations.gov>.
- E-mail: info@us-cert.gov Include the docket number "DHS-2017-0032" 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>, including any personal information provided.

SUPPLEMENTARY INFORMATION: US-CERT is responsible for performing, coordinating, and supporting response to information security incidents, which may originate outside the Federal community and affect users within it, or originate within the Federal community and affect users outside of it. Often, therefore, the effective handling of security incidents relies on information sharing among individual users, industry, and the Federal Government, which may be facilitated by and through US-CERT.

US-CERT fulfills the role of the Federal information security incident center for the United States Federal Government as defined in the Federal Information Security Modernization Act of 2014. Each Federal agency is required to notify and consult with US-CERT regarding information security incidents involving the information and information systems (managed by a Federal agency, contractor, or other source) that support the operations and assets of the agency. Additional entities report incident information to US-CERT voluntarily.

Per the Federal Information Security Modernization Act of 2014, as codified in subchapter II of chapter 35 of title 44 of the United States Code, US-CERT must inform operators of agency information systems about current and potential information security threats and vulnerabilities. Per the Homeland Security Act, as amended, the NCCIC, of which US-CERT and ICS-CERT are a part, is required to be the Federal civilian interface for sharing cybersecurity risks, incidents, analysis, and warnings for federal and non-Federal entities.

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, National Cybersecurity and Communications Integration Center, United States Computer Emergency Readiness Team

Title: Clearance for the Collection of Routine Feedback through US-CERT.gov

OMB Number: 1670-NEW

Frequency: Ongoing

Affected Public: Voluntary respondents

Number of Respondents: 126,325 respondents (estimate)

Estimated Time per Respondent: 3 minutes

Total Burden Hours: 6,140 annual burden hours

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

Total Recordkeeping Burden: \$0

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

David Epperson,

Chief Information Officer.

[FR Doc. 2017-15067 Filed: 7/17/2017 8:45 am; Publication Date: 7/18/2017]