9110-9B

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2019-0041]

Agency Information Collection Activities**:** Vulnerability Discovery Program

AGENCY: Officer of the Chief Information Security Officer, DHS.

ACTION: 60-Day Notice and request for comments; New Collection, 1601-NEW.

SUMMARY: The Department of Homeland Security, Office of the Chief Information Security Officer, will submit the following Information Collection Request (ICR) 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: You may submit comments identified by docket number DHS-2019-0041 http://www.regualtions.gov. Please follow the instructions for submitting comments.

SUPPLEMENTARY INFORMATION: Security vulnerabilities, defined in section 102(17) of the Cybersecurity Information Sharing Act of 2015, are any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control. Security vulnerability mitigation is a process starting with discovery of the vulnerability leading to applying some solution to resolve the vulnerability. There is constantly a search for security vulnerabilities within information systems, from individuals or nation states wishing to bypass security controls to gain invaluable information, to researchers seeking knowledge in the field of cyber security. Bypassing

such security controls in the DHS information systems can cause catastrophic damage including but not limited to loss in Personally Identifiable Information (PII), sensitive information gathering, and data manipulation.

Pursuant to section 101 of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act commonly known as the SECURE Technologies Act individuals, organizations, and companies will be able to submit discovered security vulnerabilities on the Department of Homeland Security (DHS) Information Systems. This collection would be used by these individuals, organizations, and companies who choose to submit a discovered vulnerability in the information system of the DHS.

The form will include the following essential information:

- Vulnerable host(s)
- Necessary information for reproducing the security vulnerability
- Remediation or suggestions for remediation of the vulnerability
- Potential impact on host, if not remediated

This form will allow the DHS to do two things 1) allow the individuals, organizations, and companies who discover vulnerabilities in the information systems of DHS to report their findings to the DHS. 2) give DHS first insight into newly discovered vulnerabilities, as well as zero-day vulnerabilities in order to mitigate the security issues prior to malicious actors acting on the vulnerability for malicious intent. The form will benefit researchers as it will provide a safe and lawful way for them to practice and discover new skills while discovering the vulnerabilities. Meanwhile, it will provide the same benefit to the DHS, in addition to enhanced information system security following

the vulnerability mitigation.

Respondents will be able to fill the form out online at https://www.dhs.gov and submit it thereafter. Links to the form will also be available at any of the DHS components websites (https://www.tsa.gov/, https://www.ice.gov/, etc.)

The collection of this information regarding to discovered security vulnerabilities by individuals, organizations, and companies is needed to fulfil the congressional mandate in Section 101 of the SECURE Technologies Act regarding a Vulnerability Disclosure Policy. In addition, without the ability to collect information on newly discovered security vulnerabilities in DHS information systems, the DHS will rely solely on the internal security personnel and or discovery through post occurrence of such a breach on security controls.

The is new collection.

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 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: The Department of Homeland Security, Officer of the Chief Information Security Officer

Title: Vulnerability Discovery Program

OMB Number: 1601-New

Frequency: On Occasion

Affected Public: Private Sector

Number of Respondents: 3000

Estimated Time Per Respondent: 3 Hours

Total Burden Hours: 9000

Dated: August 15, 2019.

Melissa Bruce,
Executive Director, Business Management Office.
[FR Doc. 2019-18576 Filed: 8/27/2019 8:45 am; Publication Date: 8/28/2019]