Agency Information Collection Activities: Vulnerability Discovery Program, 1601-0028

A Notice by the Homeland Security Department on 03/19/2021

This document has a comment period that ends in 60 days. (05/18/2021)

DOCUMENT DETAILS

Printed version:
PDF (https://www.govinfo.gov/content/pkg/FR-2021-03-19/pdf/2021-05767.pdf)

Publication Date:
03/19/2021 (/documents/2021/03/19)

Agency:
Department of Homeland Security (https://www.federalregister.gov/agencies/homeland-security-department)

Dates:
Comments are encouraged and will be accepted until May 18, 2021. This process is conducted in accordance with 5 CFR 1320.1 (/select-citation/2021/03/19/5-CFR-1320.1)

Comments Close:
05/18/2021

Document Type:
Notice

Document Citation:
86 FR 14944

Page:
14944-14945 (2 pages)

Agency/Docket Number:
Docket Number DHS-2021-0009

Document Number:
2021-05767

DOCUMENT DETAILS

DOCUMENT STATISTICS

Page views:
0
as of 03/19/2021 at 6:15 am EDT

DOCUMENT STATISTICS

PUBLISHED DOCUMENT

AGENCY:

Department of Homeland Security (DHS).

ACTION:

60-Day notice and request for comments; extension without change of a currently approved collection, 1601-0028

SUMMARY:

The Department of Homeland Security, 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 May 18, 2021. This process is conducted in accordance with 5 CFR 1320.1 (/select-citation/2021/03/19/5-CFR-1320.1)

ADDRESSES:

You may submit comments, identified by docket number Docket # DHS-2021-0009, at:

○ *Federal eRulemaking Portal: http://www.regulations.gov (http://www.regulations.gov).* Please follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name and docket number Docket # DHS-2021-0009. All comments received will be posted without change to *http://www.regulations.gov (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://ww.regulations.gov (http://ww.regulations.gov).*

SUPPLEMENTARY INFORMATION:

Controls are not always defined before being vulnerable. A better definition: 'coerces hardware/software to execute or behave in unintended ways from the design'

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

Start Printed Page 14945

~~controls to gain~~ invaluable information, to researchers seeking knowledge in the field of cyber security. Bypassing such security controls in the DHS and other Federal Agencies 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/or companies may submit any discovered security vulnerabilities found associated with the information system of any Federal agency. This collection would be used by these individuals, organizations, and/or companies who choose to submit a discovered vulnerability found associated with the information system of any Federal agency.

Specifically, DHS and Federal cybersecurity agencies are working to address the recently discovered SolarWinds hack on Federal agencies and organizations around the world. While DHS had previously obtained approval to collect this information on its own behalf, recent cyber attacks exploiting vulnerabilities have exemplified the need to have this capability government-wide. In 2020, a major cyberattack, nicknamed the SolarWinds cyberattack, by a group backed by a foreign government penetrated thousands of organizations globally including multiple parts of the United States federal government, leading to a series of data breaches. The cyberattack and data breach were reported to be among the worst cyber-espionage incidents ever suffered by the U.S., due to the sensitivity and high profile of the targets and the long duration (eight to nine months) in which the hackers had access. Affected organizations worldwide included NATO, the U.K. government, the European Parliament, Microsoft and others

Public Law 116-283 (https://www.govinfo.gov/link/plaw/116/public/283?link-type=html), Sec. 1705 (which amended 44 U.S.C. 3553 (https://www.govinfo.gov/link/uscode/44/3553?type=usc&year=mostrecent&link-type=html)) permits extensive sharing of information regarding cybersecurity and the protection of information and information systems from cybersecurity risks between Federal Agencies covered by the Federal Information Security Modernization Act and the Department of Homeland Security. This unique authority makes DHS well positioned to host the approval of this information collection on behalf of other Federal agencies

DHS is requesting pursuant to 44 US Code 3509, that the information collection be designated for any Federal agencies ability to utilize the standardized DHS online form to collect their own agency's vulnerability information and post the information on their own agency websites.

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 Federal agencies to complete the following actions; (1) allow the individuals, organizations, and/or companies who discover vulnerabilities in the information systems to report their findings to the agency, and (2) provide the agencies initial insight into any newly discovered vulnerabilities, as well as zero-day vulnerabilities in order to mitigate the security issues prior to malicious actors acting upon the vulnerability for malicious intent.

The form will also benefit researchers and will provide a safe and lawful method to practice and discover new cyber methods to discover the vulnerabilities. It will provide the same benefit to Federal agencies and will promote the enhancement of Federal information system security policies.

CLARIFY: this sounds like a safe-harbor statement for hackers

Respondents will be able to submit their information directly to ~~the agency in which they would like to report a vulnerability.~~ DHS CISA. Federal Agencies will provide the form electronically via ~~their agencies website~~. DHS common reporting web form.

vulnerability

(Have DHS manage this. One site is consistent and can be secured. Multiple agency sites will become diverse and expensive for redundant infrastructure and management. DHS has the expertise to do this right.)

The information collected does not have an impact on small business or other small entities.

The collection of this information related to the discovery of security vulnerabilities by individuals, organizations, and/or companies is needed to fulfill the congressional mandate in Section 101 of the SECURE Technologies Act related to creating Vulnerability Disclosure Policies. In addition, without the ability to collect information on newly discovered security vulnerabilities associated with Federal agency information systems, Federal agencies will rely solely on the internal security personnel and/or the discovery through a post occurrence breach of security controls.

(If you do not guarantee confidentiality, then no one will play with you. Exempt this from FOIA)

There are no assurances of confidentiality provide. Any PII that is collected will be for the sole purpose of feedback and dialogue. ~~Federal Agencies~~ DHS CISA will ensure the collection of information is covered by a Systems of Record Notice and will display a Privacy Notice to the respondents. (Again, do this right, once, at DHS CISA)

There are no changes to the information being collected.

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;

Yes. Having a notification AND FOLLOW-THROUGH remediation run by an org with expertise and expericne like CISA, will help agencies improve.

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;

Use of CISA as the central reporting agent allows the burden to be centralized and efficiencies gained from their expertise and experience.

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.

Use one site, done right, secured, and managed by those with the experience to do so. Remediation of vulnerabilities are notified, then managed by CISA. Agencies follow CISA direction to properly mitigate the vulnerabilty.

Analysis:

Agency: Department of Homeland Security, (DHS)

Title: Vulnerability Discovery Program

OMB Number: 1601-0028

Frequency: On Occasion

Affected Public: State, Local and Tribal Government

Number of Respondents: 3,000

Estimated Time per Respondent: 1 Hour

Total Burden Hours: 3,000

Robert Dorr,

Executive Director, Business Management Directorate.

[FR Doc. 2021-05767 (/a/2021-05767) Filed 3-18-21; 8:45 am]

BILLING CODE 9112-FL-P

PUBLISHED DOCUMENT