SUPPORTING STATEMENT FOR
VULNERABILITY DISCOVERY PROGRAM
OMB Control No.: 1601-0028

A. Justification

1. Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of 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 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 cyberattacks exploiting vulnerabilities have exemplified the need to have this capability government-wide. In December 2020, a major cyberattack, occurred by a group backed by a foreign government, penetrated a network monitoring tool, SolarWinds, in which impacted thousands of organizations globally, private industries, and several United States Federal Government Agencies, leading to a series of data breaches. The cyberattack was 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. Impacted organizations included NATO, the U.K. government, the European Parliament, Microsoft and others.

Pub. L. 116-283, Sec. 1705 (which amended 44 U.S.C. § 3553) 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 33554(a)(1)(B), that the information collection be designated for any Federal agency's 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.

2. Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.

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.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses, and the basis for the decision for adopting this means of collection. Also describe any consideration of using information technology to reduce burden.

Respondents may electively submit their information directly to the agency in which they would like to report a vulnerability. Federal Agencies will provide the form electronically via their agency's website.

4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purposes described in Item 2 above.

DHS has reviewed all approved collections through reginfo.gov. This information is not collected in any form, and therefore is not duplicated elsewhere. This information collection will be used across Federal Agencies to avoid duplication.

5. If the collection of information impacts small businesses or other small entities (Item 5 of OMB Form 83-I), describe any methods used to minimize burden.

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

6. Describe the consequence to Federal program or policy activities if the collection is not conducted or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

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.

7. Explain any special circumstances that would cause an information collection to be conducted in a manner:

- Requiring respondents to report information to the agency more often than quarterly;
- requiring respondents to prepare a written response to a collection of information in fewer than 30 days after receipt of it;
- requiring respondents to submit more than an original and two copies of any document;
- requiring respondents to retain records, other than health, medical, government contract, grant-in-aid, or tax records for more than three years;
- In connection with a statistical survey, that is not designed to produce valid and reliable results that can be generalized to the universe of study;
- requiring the use of a statistical data classification that has not been reviewed and approved by OMB;
- that includes a pledge of confidentiality that is not supported by authority

established in statute or regulation, that is not supported by disclosure and data security policies that are consistent with the pledge, or which unnecessarily impedes sharing of data with other agencies for compatible confidential use; or

- requiring respondents to submit proprietary trade secret, or other confidential information unless the agency can demonstrate that it has instituted procedures to protect the information's confidentiality to the extent permitted by law.

This information collection is conducted in manner consistent with guidelines in 5 CFR 13205(d)(2).

8. If applicable, provide a copy and identify the data and page number of publication in the Federal Register of the agency's notice, required by 5 CFR 1320.8(d), soliciting comments on the information collection prior to submission to OMB. Summarize public comments received in response to that notice and describe actions taken by the agency in response to these comments. Specifically address comments received on cost and hour burden.

   Describe efforts to consult with persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported.

   Consultation with representatives of those from whom information is to be obtained or those who must compile records should occur at least once every 3 years -- even if the collection of information activity is the same as in prior periods. There may be circumstances that may preclude consultation in a specific situation. These circumstances should be explained.

As required by the Paperwork Reduction Act of 1995 (PRA-95), the Agency issued a 60 Day Federal Register notice on March 19, 2021 at 86 FR 14944, soliciting comments from the public on the information collection. DHS received three comments, two were non-substantive, and one comment is discussed below. No changes are being made as a result of the comments.

<u>Comment 1:</u> In this notice DHS continues to rely on the 'information sharing' provisions of 44 USC 3553(l) (added by §1705(2) 1705 of PL 116-283). This language allows DHS to "access, use, retain, and disclose, and the head of an agency may disclose to the Secretary, information, for the purpose of protecting information and information systems from cybersecurity risks." That does not really pertain to collecting voluntarily supplied information from outside of the government for a vulnerability discover program.

<u>DHS Response</u>: DHS concurs. The provisions of 44 USC 3553 provide that the Secretary of Homeland Security shall issue binding operational directives to agencies to ensure compliance with Federal Information Security

Management Act of 2002 (FISMA). On September 2, 2020, the Cybersecurity and Infrastructure Security Agency (CISA), on behalf of the Secretary required agencies to stand up Vulnerability Disclosure Policies through a Binding Operational Directive 20-01. Agencies, in turn, are required by 44 USC 3554(a)(1)(B) to comply with such requirements. Thus, the information collection from the public is mandatory for agencies.

<u>Comment 2:</u> It only seems reasonable to assume that a multi-agency VDP would have a larger number of responses, burden and cost.

<u>DHS Response</u>: DHS is not able to project the multi-agency burden at the current time. The VDP Program is still in its early stages. DHS will reevaluate the burden in the upcoming year(s) and will notify the public of future burden estimate modifications.

As required by the Paperwork Reduction Act of 1995 (PRA-95), the Agency issued a 30-Day Federal Register notice on August 23, 2021 at 86 FR 41, soliciting comments from the public on the information collection requirements contained in the DHS form.

9. Explain any decision to provide any payment or gift to respondents, other than remuneration of contractors or grantees.

No Federal Agency will provide payments or gifts to respondents.

10. Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy.

There are no assurances of confidentiality provide. Any PII that is collected will be for the sole purpose of feedback and dialogue. Federal Agencies will ensure the collection of information is covered by a Systems of Record Notice and will display a Privacy Notice to the respondents.

11. Provide additional justification for any questions of a sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private. This justification should include the reasons why the agency considers the questions necessary, the specific uses to be made of the information, the explanation to be given to person's form whom the information is requested, and any steps to be taken to obtain their consent.

The are no questions of sensitive nature.

12. Provide estimates of the hour burden of the collection of information. The statement should:

- Indicate the number of respondents, frequency of response, annual hour burden, and an explanation of how the burden was estimated. Unless directed to do so, agencies should not conduct special surveys to obtain information on which to

base hour burden estimates. Consultation with a sample (fewer than 10) of potential respondents is desirable. If the hour burden on respondents is expected to vary widely because of differences in activity, size, or complexity, show the range of estimated hour burden, and explain the reasons for the variance. Generally, estimates should not include burden hours for customary and usual business practices.

- If this request for approval covers more than one form, provide separate hour burden estimates for each form and aggregate the hour burdens in Item 13 of OMB Form 83-I.

- Provide estimates of annualized cost to respondents for the hour burdens for collections of information, identifying and using appropriate wage rate categories. The cost of contracting out or paying outside parties for information collection activities should not be included here. Instead, this cost should be included in Item 14.

Type of Respondent	Form Name / Form Number	No. of Respondents	No. of Responses per Respondent	Avg. Burden per Response (in hours)	Total Annual Burden (in hours)	Avg. Hourly Wage Rate	Total Annual Respondent Cost
Individuals (No affiliation)	VDP form	1,000	1	3.0	3,000	$71.92	215,760
Organizations	VDP form	1,000	1	3.0	3,000	$71.92	215,760
Companies	VDP form	1,000	1	3.0	3,000	$71.92	215,760
Total		3,000			9,000		647.280

**This figure reflects an estimate for the total number of respondents*

***Individuals are anyone who is not affiliated to any company or organization and participates in the VDP self-willingly*

**** Organizations include government organizations such as educational institutions, or other non-government organizations including cyber related organizations*

~The above Average Hourly Wage Rate is the May 2018 Bureau of Labor Statistics average wage for Information Security Analysts Occupations of $49.26 times the wage rate benefit multiplier of 1.46 (to account for benefits provided) equaling $71.92 The selection of "Information Security Analysts" was chosen as the expected respondents for this collection could be expected to be from this occupation.

** These burden estimates will be updated upon the next submission of this Information Collection Request to OMB for review and approval.*

13. Provide an estimate of the total annual cost burden to respondents or record keepers resulting from the collection of information. (Do not include the cost of any hour burden shown in Items 12 and 14).

- The cost estimate should be split into two components: (a) a total capital and start-up cost component (annualized over its expected useful life); and (b) a total operation and maintenance and purchase of services component. The estimates

should consider costs associated with generating, maintaining, and disclosing or providing the information. Include descriptions of methods used to estimate major cost factors including system and technology acquisition, expected useful life of capital equipment, the discount rate(s), and the time period over which costs will be incurred. Capital and start-up costs include, among other items, preparations for collecting information such as purchasing computers and software; monitoring, sampling, drilling and testing equipment; and record storage facilities.

- If cost estimates are expected to vary widely, agencies should present ranges of cost burdens and explain the reasons for the variance. The cost of purchasing or contracting out information collection services should be a part of this cost burden estimate. In developing cost burden estimates, agencies may consult with a sample of respondents (fewer than 10), utilize the 60-day pre-OMB submission public comment process and use existing economic or regulatory impact analysis associated with the rulemaking containing the information collection, as appropriate.

- Generally, estimates should not include purchases of equipment or services, or portions thereof, made: (1) prior to October 1, 1995, (2) to achieve regulatory compliance with requirements not associated with the information collection, (3) for reasons other than to provide information or keep records for the government or (4) as part of customary and usual business or private practices.

  There are no record keeping, capital, start-up or maintenance cost associated with this collection.

14. Provide estimates of annualized cost to the Federal government. Also, provide a description of the method used to estimate cost, which should include quantification of hours, operational expenses (such as equipment, overhead, printing, and support staff), and any other expense that would not have been incurred without this collection of information. Agencies also may aggregate cost estimates from Items 12, 13, and 14 in a single table.

The total estimated cost for the government is based on the collection, review, validation, and distribution of data. The collection lifecycle involves the following process 1) Review of collected submissions for completeness 2) reproduction of the discovered vulnerability to validate its' usefulness 3) distribution of validated security vulnerabilities report to components. The cost is calculated by multiplying the estimated number of respondents by the estimated time to collection completion (review, validation and distribution) and multiplying this by the average information security government employee salary (3,000 estimated responses/yr. x 3.5hrs time to validation x $82.26/hr. the average GS-14 salary $56.34/hr. x 1.46 (wage rate benefit multiplier) = total of $863,730/yr.). The total cost for the federal government is $863,730/yr.

15. Explain the reasons for any program changes or adjustments reporting in Items 13 or 14 of the OMB Form 83-I.

No adjustments in the estimates are being made to the current burden.

16. For collections of information whose results will be published, outline plans for tabulation, and publication. Address any complex analytical techniques that will be used. Provide the time schedule for the entire project, including beginning and ending dates of the collection of information, completion of report, publication dates, and other actions.

Federal Agencies do not intend to employ the use of statistics or the publication thereof for this information collection.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons that display would be inappropriate.

Federal Agencies will display the expiration date for OMB approval of this information collection.

18. Explain each exception to the certification statement identified in Item 19, "Certification for Paperwork Reduction Act Submission," of OMB 83-I.

DHS did not request an exception to the certification of this information.