Supporting Statement for Paperwork Reduction Act Submission

Nationwide Cyber Security Review (NCSR) Assessment

OMB Control Number: DHS-1670-NEW

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.

In reports to the Department of Homeland Security (DHS) Appropriations Act, 2010, Congress requested a Nationwide Cyber Security Review (NCSR) from the National Cyber Security Division (NCSD), the predecessor organization of the Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) division. S. Rep. No. 111-31, at 91 (2009), H.R. Rep. No. 111-298, at 96 (2009). The House Conference Report accompanying the Department of Homeland Security Appropriations Act, 2010, "note[d] the importance of a comprehensive effort to assess the security level of cyberspace at all levels of government" and directed DHS to "develop the necessary tools for all levels of government to complete a cyber network security assessment so that a full measure of gaps and capabilities can be completed in the near future." H.R. Rep. No. 111-298, at 96 (2009). Concurrently, in its report accompanying the Department of Homeland Security Appropriations Bill, 2010, the Senate Committee on Appropriations recommended that DHS "report on the status of cyber security measures in place, and gaps in all 50 States and the largest urban areas." S. Rep. No. 111-31, at 91 (2009).

The Homeland Security Act of 2002, as amended, established "a national cybersecurity and communications integration center [which is commonly known as the NCCIC]… to carry out certain responsibilities of the Under Secretary," including the provision of assessments. 6 U.S.C. § 148(b). The Act also directs the composition of the NCCIC to include an entity that collaborates with State and local governments on cybersecurity risks and incidents, and has entered into a voluntary information sharing relationship with the NCCIC. 6 U.S.C. § 148(d)(E). The Multistate Information Sharing and Analysis Center (MS-ISAC) currently fulfills this function. The DHS Cybersecurity and Infrastructure Security Agency (CISA) funds the MS-ISAC through a Cooperative Agreement and maintains a close relationship with this entity. As part of the Cooperative Agreement, DHS directs the MS-ISAC to produce the NCSR as contemplated by Congress.

Generally, CISA has authority to perform risk and vulnerability assessments for federal and non-federal entities, with consent and upon request. The NCCIC performs these assessments in accordance with its authority to provide voluntary technical assistance to federal and non-federal entities. *See* 6 U.S.C. §§ 148(c)(6), 143(2). This authority is consistent with the Department's

responsibility to "[c]onduct comprehensive assessments of the vulnerabilities of the Nation's critical infrastructure in coordination with the SSAs [Sector Specific Agencies] and in collaboration with SLTT [State Local Tribal and Territorial] entities and critical infrastructure owners and operators." PPD-21, at 3. A private sector entity or State and local government agency also has discretion to use a self-assessment tool offered by CISA or request CISA to perform an on-site risk and vulnerability assessment. *See* 6 U.S.C. §§ 148(c)(6), 143(2); 6 U.S.C. § 121(d)(2). The NCSR is a voluntary annual self-assessment.

Upon submission of the first NCSR report in March 2012, Congress further clarified its expectation "that this survey will be updated every other year so that progress may be charted and further areas of concern may be identified." S. Rep. No. 112-169, at 100 (2012). In each subsequent year, Congress has referenced this NCSR in its explanatory comments and recommendations accompanying the Department of Homeland Security Appropriations. Consistent with Congressional mandates, SECIR developed the NCSR to measure the gaps and capabilities of cybersecurity programs within state, local, tribal and territorial (SLTT) governments. Using the anonymous results of the NCSR, DHS delivers a bi-annual summary report to Congress that provides a broad picture of the current cybersecurity gaps and capabilities of SLTT governments across the nation.

The assessment allows SLTT governments to manage cybersecurity related risks through the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) which consists of best practices, standards, and guidelines. In efforts of continuously providing Congress with an accurate representation of the SLTT governments' cybersecurity programs gaps and capabilities, the NCSR question sets and surveys may slightly change from year to year to accurately reflect the current cybersecurity environment.

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 NCSR is an annual voluntary self-assessment that is hosted on the RSA Archer Suite. The self-assessment runs every year from October through December. In efforts of increasing participation, the deadline is sometimes extended.

The target audience for the NCSR are personnel within the SLTT community who are responsible for the cybersecurity management within their organization.

Through the NCSR, DHS & MS-ISAC will examine relationships, interactions, and processes governing IT management and the ability to effectively manage operational risk. Using the anonymous results of the NCSR, DHS delivers a bi-annual summary report to Congress that provides a broad picture of the cybersecurity gaps and capabilities of SLTT governments across the nation.

The bi-annual summary report is shared with MS-ISAC members, NCSR End Users, and

Congress. The report is also available on the MS-ISAC website.

Upon submission of the NCSR self-assessment, participants will immediately receive access to several reports specific to their organization and their cybersecurity posture. Additionally, after the annual NCSR survey closes there will be a brief NCSR End User Survey offered to everyone who completed the NSCR assessment. The survey will provide feedback on participants' experiences, such as how they heard about the NCSR, what they found or did not find useful, how they will utilize the results of their assessment, and other information about their current and future interactions with the NCSR.

Additionally, MS-ISAC will administer a survey to those who were registered participants in the past and did not register or complete the most recent NCSR. The purpose of the Non-Response Survey is to solicit feedback on ways the NSCR could be improved to maximize benefits and increase response rates in the future.

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.

The assessment, located on the RSA Archer Suite, requires approximately two hours for completion (per organization). All information provided through the platform will not use any additional forms of information technology other than what is provided via the RSA Archer Suite. During the assessment period, participants can respond at their own pace with the ability to save their progress during each session. If additional support is needed, participants can contact the NCSR helpdesk via phone and/or email.

The NCSR End User survey will be fully electronic. It contains less than 30 multiple choice and fill-in-the-blank answers and takes approximately 10 minutes to complete. The feedback survey will be administered via Survey Monkey and settings will be updated to opt out of collecting participants' IP addresses.

The Non-Response Survey will be fully electronic and take approximately 10 minutes to complete. The survey will be administered via Survey Monkey and settings will be updated to opt out of collecting participants' IP addresses.

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.

Through the NCSR, DHS and MS-ISAC will examine relationships, interactions, and processes governing IT management and the ability to effectively manage operational risk within the

SLTT community. Each assessment respondent is considered an independent entity, whereby they answer the survey questions as they relate to their organization for that specific year. The concept of duplication is not relevant to the NCSR. Also, a search of reginfo.gov revealed that this information is not collected in any form, and therefore is not duplicated elsewhere.

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 NCSR is a voluntary self-assessment of the IT services of state, local, tribal and territorial governments. This information collection does not have an impact on small businesses 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.

MS-ISAC & DHS conducts the NCSR self-assessment on an annual basis, from October through December. DHS uses the anonymous results of the NCSR to deliver a bi-annual summary report to Congress that provides a broad picture of the cybersecurity programs gaps and capabilities of SLTT governments across the nation. Awareness and knowledge of existing capabilities and subsequent gaps is in turn used to directly address and support DHS' cybersecurity goal of analyzing and reducing cyber threats and vulnerabilities. Without this information, SECIR would not be able to support the DHS cybersecurity mission of threat and vulnerability reduction, and would not be able to meet the statutory requirement to deliver the bi-annual Congressional report. (Upon submission of the first NCSR report in March 2012, Congress further clarified its expectation "that this survey will be updated every other year so that progress may be charted and further areas of concern may be identified." S. Rep. No. 112-169, at 100 (2012). Additionally, participants would not have access to information critical to their cybersecurity posture improvement.

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;**

The special circumstances contained in item 7 of the Supporting Statement are not applicable to this information collection.

- **Requiring respondents to prepare a written response to a collection of information in fewer than 30 days after receipt of it;**

NCSR respondents will not provide written responses within less than 30 days. The assessment

consists of check-boxes and dropdown menus. The assessment takes place annually from October through December. Respondents have the ability to save their progress and log back into the RSA Archer Suite to submit their assessment anytime during October and December while the assessment is open.

- **Requiring respondents to submit more than an original and two copies of any document;**

Respondents are only permitted to submit their assessment one time. This will be enforced through the RSA Archer Suite.

- **Requiring respondents to retain records, other than health, medical, government contract, grant-in-aid, or tax records for more than three years;**

The special circumstances contained in item 7 of the Supporting Statement are not applicable to this information collection.

- **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;**

Upon submission of the self-assessment, participants will immediately receive access to several reports specific to their organization and their cybersecurity posture. (Discussed in question 2). At the conclusion of the assessment period, MS-ISAC & DHS will aggregate all assessment data and conduct a more in-depth statistical analysis across the participants. The Congressional Report will ensure non-attribution (will not identify single respondents in the report) and is available for all respondents, MS-ISAC members and Congress.

- **Requiring the use of a statistical data classification that has not been reviewed and approved by OMB;**

The special circumstances contained in item 7 of the Supporting Statement are not applicable to this information collection.

- **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**

All information will be protected by the existing security controls of the US-CERT.gov system. . For defensive measures and indicators shared under CISA, Federal entities are required to apply appropriate controls to protect the confidentiality of cyber threat indicators that contain personal information of a specific individual or information that identifies a specific individual that is directly related to a cybersecurity threat or a use authorized under CISA to the

greatest extent practicable. 6 U.S.C. § 1504(b).

- **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.**

The NCSR survey does not request trade secrets, confidential, or classified information. This assessment is voluntary.

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.

	Date of Publication	Volume #	Number #	Page #	Comments Addressed
60-Day Federal Register Notice:	Thursday, July 5, 2018	83	129	31412	No comments received.
30-Day Federal Register Notice	Wednesday, October 17, 2018	83	201	52499	No comments received.

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

Using funds from the Center for Internet Security (CIS), the MS-ISAC encourages participation by randomly selecting up to 10 NCSR respondents who completed the self-assessment in full to receive a $50.00 gift card.

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

In inviting stakeholders to participate, the MS-ISAC characterizes the NCSR as a free and confidential assessment and that it allows stakehodlers to participate anonymously. For defensive measures and indicators shared under CISA, Federal entities are required to apply appropriate controls to protect the confidentiality of cyber threat indicators that contain personal information of a specific individual or information that identifies a specific individual that is

directly related to a cybersecurity threat or a use authorized under CISA to the greatest extent practicable. 6 U.S.C. § 1504(b).

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.

There are no questions of a 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**

The NCSR is a voluntary self-assessment designed to measure the gaps and capabilities of cybersecurity programs within state, local, tribal and territorial governments. As it is voluntary, we do not know the number of potential respondents. To estimate the number of respondents, we looked at past participation to forecast what participation in the next three years would be. We then took the average of the three year projection as our estimated annual respondents. This gave us an estimated 590 annual respondents. Table 1 presents the estimated number of respondents, based on historical data.

Table 1: Self-Assessment Participation

Year	Percent of Participation	Number of Respondents
2011	0.18%	162
2013	0.34%	304
2014	0.28%	252
2015	0.41%	365
2016	0.52%	464
2017	0.53%	476
2018	0.60%	536
2019	0.66%	590
2020	0.72%	644
2018-2019 Average		590

We estimate that the NCSR Assessment will take no longer than two hours to complete (data collected in post survey question) per organization.

For an estimated 590 annual respondents, the burden is 1,179 (2 hrs x 590 respondents) hours. To estimate the annual cost burden of the NCSR Assessment, we multiply the total number of respondents by 2 burden hours, resulting in a total of 1,179 burden hours. We then multiply this by the mean loaded hourly wage for all occupations in the professional, scientific, and technical service sector, per BLS. The fully loaded wage is calculated by multiplying the mean wage of $38.32[1] by the load factor of 1.38869, for a fully loaded wage rate of $53.21[2]. At a rate of $53.21 per hour, the dollar value of the total annual burden hours associated with the existing elements of this information collection equals $62,765.

Additionally, MS-ISAC will be issuing an end-user survey along with the NCSR Assessment, to be filled out as well. We estimate that the end-user survey will take approximately 10 minutes to complete and will be completed by all 590 respondents for a total of 98 burden hours and a burden cost of $5,230.[3]

A third instrument will also be distributed by the MS-ISAC, which is a non-response survey that will be sent to 100 participants registered in the past and did not register or complete the most recent NCSR. The average response rate to the NCSR since 2011 has been 0.47%. As such, for this ICR, we anticipate a 1% response rate to this non-response survey. The non-response

1 Sector 54 Professional, Scientific, and Technical Services, All Occupations. https://www.bls.gov/oes/may/2017/naics2_54.htm

2 The load factor is determined by dividing the total compensation by the wages and salaries for all private industry workers in the Professional, Scientific, and Technical Services sector, using 2016 BLS data.

3 Burden cost will be the product of the burden hours (98) multiplied by the same fully loaded wage rate ($53.21) used to estimate the cost of the NCSR Survey.

survey will take an estimated 10 minutes to complete, and we expect 1 annual respondent, for a cost of $9, using the same estimation methodology as used for the end-user survey.

Instrument	Respondents	# of Respondents	Responses per Respondent	Total Annual Number of Responses	Average Burden per Response (in hours)	Total Annual Burden (in hours)	Average Hourly Wage(in dollars)	Total Annual Burden (in dollars)
NCSR Assessment	CIOs, CISOs, IT Managers within SLTT governments	590	1	590	2	1,180	$53.21	$62,765
End User Survey	CIOs, CISOs, IT Managers within SLTT governments	590	1	590	0.167	98	$53.21	$5,230
Non-Response Survey	CIOs, CISOs, IT Managers within SLTT governments	1	1	1	0.167	0	$53.21	$9
Total		**1,181**		**1,181**		**1,278**		**$68,005**

For all three instruments, we estimate a total burden of 1,278 hours for a total cost of $68,005 (1,278 hours x $53.21).

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 take into account 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 recordkeeping, capital, start-up, or maintenance costs associated with this information collection. There is no submission or filing fee associated with this collection. As all forms are completed via the US-CERT.gov portal, there are no associated collection, printing, or mailing costs.

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.

SECIR and MS-ISAC are utilizing existing technologies and capabilities to execute the NCSR. The NCSR question set is based off of the NIST CSF and is currently being hosted on the RSA Archer Suite.

Based on internal review, NCSD personnel estimate that it takes approximately four hours to review the NCSR assessment data and create the associated Congressional Report. The four hours is divided equally among government GS-scale employees and contracted workers. There are 590 responses that will require a review, for a total burden of 2,359 hours. For both the government and contracted workers, we use the GS13 step 5 in the Washington, D.C. area wage rate as the basis of our cost estimate. For 2018, the GS13 step 5 base salary is $109,900[4] per year, which we convert to an hourly wage by dividing by 2080 hours for a full time employee, for an hourly wage of $52.84. We then multiply the hourly wage by a load factor of 1.4639[5] to

4 https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2018/DCB.pdf

5 Load factor based on BLS Employer Cost for Employee Compensation, as of June 9, 2017. Load factor = Employer cost for employee compensation ($35.28) / wages and salaries ($24.10) = 1.4639 https://www.bls.gov/news.release/ecec.nr0.htm

account for benefits and non-salary compensation. The loaded wage rate is $77.35, which we then multiply by the total burden hours of 2,359 for a total cost to the government of $182,459.

Data for **590** Respondents x **4** hours/per respondent = **2,359** hours to review data

2,359 hours x $77.35 = $ 182,459

Total Cost to the Government = $182,459

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

This is a collection in use without an OMB Control Number and is being brought into compliance with the Paperwork Reduction Act.

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.

All SLTT Respondents will be required to submit their data by the deadline provided. December timeline for the NCSR analysis and reporting is below:

NCSR Analysis and Reporting

a. Every respondent will receive access to individual reports immediately after they submit the assessment
    i. Individual Reports will be available on the NCSR Dashboard which is housed on the RSA Archer Suite.
b. MS-ISAC/DHS will provide a "Congressional Report" after the survey period
    i. Audience: Congress (access to report given to NCSR participants for comparison purposes & MS-ISAC members)
    ii. The Congressional Report is shared with MS-ISAC members, NCSR End Users, and Congress. The report is also available on the MS-ISAC website and will include:
        1. Introduction and series of disclaimers/copyrights
        2. Reporting methodology
        3. Year-to-Year scoring by peer groups:
            a. Comparison made amongst States
            b. Comparison made amongst Locals
            c. Comparison made amongst Tribes
            d. Comparisons made amongst Sub-Sectors (This is a new addition as of 2018. New sub-sector groups include but are not limited to: State Health & Human Services,

County/Parish, State Business/Administration, State Environment, State Public Safety, State Elections, etc.)

i. June – July: Perform updates/modifications to refine the assessment survey (questions/answers/recommendations)
ii. August – October: Marketing the NCSR to SLTT entities and registering new users to the platform
iii. October – December: Respondents will have access to complete and or edit the current year's survey during the months of October through December. Each respondent will have access to several individualized reports following the submission of their survey. The individualized report will be automatically generated (using technologies on the RSA GRC Platform). Respondents are able to download and export the reports.
iv. January – March: MS-ISAC will begin analyzing all data received from completed surveys and perform statistical analysis.
v. April – May: MS-ISAC will work to finalize the Congressional Report.
vi. May – July: DHS will approve the Congressional Report. The Congressional Report will be made available to all assessment Respondents for comparison purposes (comparing the Individualized Report to the Congressional Report) and MS-ISAC members. As the NCSR is a Congressional request, the Congressional Report will also be shared to Congress. It is important to note that DHS will ensure non-attribution and not identify the "scores or ratings" of states or SLTT governments in the Congressional Report.
    a. The bi-annual summary report is shared with MS-ISAC members, NCSR End Users, and Congress. The report is also available on the MS-ISAC website.

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.

CISA 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.

CISA does not request an exception to the certification of this information collection.