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.

Per the House Report 111-298 and Senate Report 111-31, the National Cyber Security Division (NCSD), Cyber Security Evaluation Program (CSEP) has been tasked to develop a nationwide assessment in order to evaluate the cybersecurity posture of all 50 States and 64 Large Urban Areas (outlined in FEMA's Urban Area Security Initiative). The actual NCSR assessment will be initiated by an automated survey via secure portal (US-CERT). The voluntary survey will allow states and large urban areas (LUAs) to assess themselves based on an existing NCSD cybersecurity assessment framework. See "Attachment *1_House and Senate Requirements.doc"* for more information. The NCSR questions have also been attached, *"Attachment 2_NCSR Questions_Feb 10 2011.doc."*

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 a voluntary self-assessment of the Information Technology (IT) services of State and Large Urban Area (LUA) governments, designed to measure cyber security preparedness and resilience. Through the NCSR, CSEP will examine relationships, interactions, and processes governing IT management and the ability to effectively manage operational risk. The NCSR seeks to elicit involvement from Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Chief Technology Officers (CTOs), and IT Security personnel. Upon submission of the assessment, participants will immediately receive a report containing IT resilience analysis and options for consideration to improve an organization's cyber security posture. At the conclusion of the assessment period, CSEP will aggregate all assessment data and conduct more in-depth statistical analysis and benchmarking across the participants.

Each respondent of the NCSR assessment will receive an individualized report (automatically generated after the assessment), which will outline areas for improvement, provide best practices, and references to other notable resources. Once all data has been analyzed, CSEP will

create a Congressional Report that contains the benchmarks and statistical analysis of all NCSR Respondents (ensuring non-attribution in the Congressional Report).

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 US-CERT Secure Portal, requires approximately two hours for completion (per respondent). All information provided through the portal is safeguarded in accordance with the DHS Protected Critical Infrastructure Information program (http://www.dhs.gov/PCII). The assessment will not use any additional forms of information technology, other than, what is provided via the US-CERT portal. During the assessment period, participants can respond at their own pace with the ability to save their progress during each session. Instructions and clarifying guidance are included in the assessment tool. If additional support is needed, participants can contact the NCSR helpdesk via phone and email.

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, CSEP will examine relationships, interactions, and processes governing IT management and the ability to effectively manage operational risk within States and Large Urban Areas. Each assessment Respondent is considered an independent entity, whereby they answer the survey questions as they relate to their organization. The concept of duplication is not relevant to the NCSR.

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.**

There is no burden on small businesses or other small entities. The NCSR is a voluntary self-assessment of the Information Technology (IT) services of State and local governments.

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.**

CSEP will conduct the NCSR assessment during National Cybersecurity Awareness Month in October 2011. Other than October 2011, the frequency of NCSR assessments has yet to be determined. We envision the NCSR to take place annually, but we are waiting on clarification from Congress.

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;**

See the response in Section 6, above.

- **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. The assessment consists of check-boxes and radio buttons. The assessment will take place from October 1-31, 2011. Respondents have the ability to save their progress and log back into the US-CERT portal to submit their assessment within the month of October.

- **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 US-CERT portal.

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

Not applicable to the NCSR.

- **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;**

Results will be outlined in two reports. Upon submission of the assessment, participants will immediately receive a report containing IT resilience analysis and options for consideration to improve an organization's cyber security posture. At the conclusion of the assessment period, CSEP will aggregate all assessment data and conduct more in-depth statistical analysis and benchmarking across the participants. The Congressional Report will ensure non-attribution (will not identify single Respondents in the report) and is available for all Respondents and Congress.

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

Not applicable to the NCSR. All results will be classified as PCII.

- **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. Data obtained through the NCSR survey will be classified as PCII.

- **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
60Day Federal Register Notice:	April 21, 2011	76	77	22409	No comments received.
30-Day Federal Register Notice	July 21, 2011	76	140	43696	No comments received.

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

Not applicable to the NCSR. The NCSR assessment is not associated with monetary value.

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

The NCSR survey resides on the US-CERT.gov's Secure Portal. This system has been certified and accredited at the Moderate level. All data collected through the NCSR assessment will be

protected by PCII. All Department information systems are audited regularly to ensure appropriate use and access to information. Authorized users must supply a valid log-on and password to obtain access to the US-CERT Portal. Within DHS, access to portal resources and member information is limited to those who require it for completion of their official duties. Portal administrators periodically review shared spaces to ensure that postings by its members do not contain sensitive PII or PII about those who are not members or potential members of the online community. Administrators have the ability to remove any inappropriate postings.

All Department employees and contractors are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of PII such as what is contained in portals.

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.

Not applicable to the NCSR. The NCSR is a voluntary self-assessment of the Information Technology (IT) services of State and Large Urban Area (LUA) governments, designed to measure cyber security preparedness and resilience.

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 of the Information Technology (IT) services of State and Large Urban Area (LUA) governments, designed to measure cyber security preparedness and resilience. As it is voluntary, we do not know the number of potential Respondents. It is estimated that 500-1000 IT Professionals in State and local Governments will participate. The survey will take no longer than 2 hours to complete (validated through pilot activities and industry feedback) per respondent. As the NCSR is voluntary, it is difficult to predict the true number of respondents. We expect 500-1000 respondents, so the numbers below are associated with 750 respondents.

For an estimated 750 respondents, the burden is 1500 (2hrs x 750 respondents) hours. At a rate of $24.42 per hour[1], the dollar value of the total annual burden hours associated with the existing elements of this information collection equals $36,630.00.

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 50 States and 64 Large Urban Areas	750	1	750	2	1500	$24.42	$36,630

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**

1 This hourly rate is an average hourly wage calculation based on Bureau of Labor Statistics (BLS) from May 2008 for numerous occupations of persons who attend OEC events, including the following: Medical and Health Services Managers; Emergency Management Specialists; Network and Computer Systems Administrators; Network Systems and Data Communications Analysts; Electrical and Electronic Engineering Technicians; Emergency Medical Technicians and Paramedics; First-Line Supervisors/Managers of Police and Detectives; First-Line Supervisors/Managers of Police and Detectives; First-Line Supervisors/Managers of Fire Fighting and Prevention Workers; First-Line Supervisors/Managers; Protective Service Workers (All Other); Fire Fighters; Police and Sheriff's Patrol Officers; Sales Representatives (Wholesale and Manufacturing, Technical and Scientific Products); Communications Equipment Operators (All Other); Reservation and Transportation Ticket Agents and Travel Clerks; Police, Fire, and Ambulance Dispatchers; Dispatchers (Except Police, Fire, and Ambulance); Legal Secretaries; Medical Secretaries; Secretaries (except Legal, Medical, and Executive); First-Line Supervisors/Managers (of Mechanics, Installers, and Repairers); Radio Mechanics; Telecommunications Equipment Installers and Repairers (except Line Installers); US Government Employee (GS-13, Step 5, averaged across locality and CONUS).

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.**

Not applicable to the NCSR. 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.**

The Cyber Security Evaluation Program (CSEP) is utilizing existing technologies and capabilities to execute the NCSR. Our survey questions already exist as part of our Cyber Resilience Review (CRR) assessment framework. The survey questions are simply being added to the US-CERT.gov's Security Portal in order to centrally disseminate to our industry Respondents. All data captured as a result of the survey will be stored on the existing US-CERT.gov portal.

Based on internal review, NCSD personnel estimate that it takes approximately 4 hours to review the NCSR assessment data and create the associated Congressional Report. An average

base salary of $104.07/hour for contract support staff and Program Analysts Grade 13 step 5 was used for these calculations.

Data for **750** Respondents x **2** hours/per Respondent= **1500** hours to review data

1500 hours x $104.07 = $ 156,105

Total Cost to the Government = $156,105

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 new collection.

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 Respondents (States and LUAs) will be required to submit their data by October 31, 2011. The timeline for the NCSR analysis and reporting is below:

NCSR Analysis and Reporting

a. All Data Submitted will be protected under PCII
b. Every respondent will receive an "Individual Report" immediately after they submit the assessment
    i. The Individual Report will include:
        1. Introduction and series of disclaimers/copyrights/CMU no warranty
        2. Reporting methodology
        3. The questions
        4. How the respondent answered each question
        5. A score for each question
        6. High level options for consideration based on answers
    ii. Individual Report will be uploaded to the private Document Library of each respondent's account
c. CSEP will provide a "Congressional Report" after the survey period
    i. Audience: Congress (access to report given to NCSR participants for comparison purposes)
    ii. The Congressional Report will include:
        1. Introduction and series of disclaimers/copyrights
        2. Reporting methodology
        3. Benchmarking
            a. Comparison made amongst States

b. Comparison made amongst State Agencies:
    i. Across the Nation
    ii. Within each State
c. Comparison made amongst LUAs:
    i. Across the Nation
    ii. Within each State

i. July—Sept 2011: Perform updates/modifications to refine the assessment survey (questions/answers/recommendations)
ii. October 1-31, 2011: Respondents will only have access to the survey during the month of October 2011. Each Respondent will receive an "Individualized Report" following the submission of their survey. The Individualized Report will be automatically generated (using technologies on the US-CERT.gov Portal) and uploaded into the Document Library of each Respondent.
iii. November —January 2012: CSEP will begin analyzing all data received from completed surveys and perform benchmarking and statistical analysis.
iv. February—March 2012: CSEP will work to finalize 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). As the NCSR is a Congressional request, the Congressional Report will also be shared to Congress. It is important to note that CSEP will ensure non-attribution and not identify the "scores or ratings" of states or LUAs in the Congressional Report.

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.

Not applicable. The OMB Control No. "DHS-1670-NEW" will be identified on the NCSR assessment.

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

NCSD, CSEP does not request an exception to the certification of this information collection.