United States Department of Energy
Supporting Statement A
"Electric Sector Cybersecurity Risk Management Maturity Initiative"
OMB Number 1910-New

A. Justification

This supporting statement provides additional information regarding the Department of Energy (DOE) request for processing of the emergency proposed information collection, Electric Sector Cybersecurity Risk Management Maturity Initiative. The numbered questions correspond to the order shown on the Office of Management and Budget (OMB) Form 83-I, "Instructions for Completing OMB Form 83-I."

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.

Increasing cyber threats to the security of the nation's electric grid could have dramatic effects on the physical and economic security of the Nation. It is the responsibility of the Department of Energy, under the authorities and responsibilities granted by Homeland Security Presidential Directive 7 (HSPD-7), to "collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms." It is imperative that the owners and operators of the nation's electric utilities, as well as the government agencies supporting the sector, have the ability to understand what capabilities and competencies will allow the sector to defend itself, and how to prioritize necessary investments. The Department of Energy, at the request of the White House, and in collaboration with the Department of Homeland Security and industry experts, is developing a maturity model in a collaborative partnership with owners, operators, and subject matter experts to meet their request to identify and prioritize capabilities relative to risk and cost.

The model includes 10 domains, or logical groupings of cybersecurity risk management activities. In the domain descriptions, "critical infrastructure" includes government concerns about the grid (like those driving this effort), and "organizational objectives" take into account privacy, product quality, and other utility stakeholder concerns. The current draft of the model also includes four maturity indicator levels (MILs) which are defined by sets of generic guidelines that describe the nature, completeness, and institutionalization of the practices in a domain at that MIL. An assessment tool, consisting of multiple choice questions which measure a participant's implementation of characteristics or practices that form the sets of activities correlated to MILs will be used to collect the information. Feedback on the tool's ease of use, relevance and applicability from the participants in the pilot will allow DOE to revise and validate the capabilities of the model. Successful development of a model which has been validated by industry and is ready for deployment in the electric sector will satisfy the request from the White

House to create the capability to understand the maturity of cybersecurity across the electric sector.

This collection of information is necessary in order for DOE to serve the needs of electric sector owners and operators, and to comply with the request from the White House to assess the cybersecurity maturity of the sector. While we recognize there are other assessments and models in use to assess cybersecurity capabilities, there is not currently a capability model that addresses the specific characteristics of the electric sector.

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 Department will use the information to identify areas of improvement for the model and evaluation tool. Feedback on the tool's ease of use, relevance and applicability from the participants in the pilot will allow DOE to revise and validate the capabilities of the model and evaluation tool.

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.

Pilot participants will fill out the assessment tool and receive their results electronically through the use of a fill-able PDF on site using their own equipment. The electronic version of the tool will be delivered to the participants via email. DOE has requested that participants submit their information electronically through their respective trade organizations, who will in turn submit information to DOE electronically utilizing DHS' Protected Critical Infrastructure Information (PCII) submission process, which also occurs via email. The Department has concluded this is the least burdensome process for the participants.

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.

The DOE team has gone through a long and exhaustive process to identify other maturity models and assessment programs used throughout the sector and by other partners. These activities were then assessed by a team of volunteers from DOE, industry, partner agencies and subject matter experts to assess their applicability to the electric sector and the goals of the Electric Sector Cybersecurity Risk Management Maturity Initiative.

While portions of existing programs and best practices have been incorporated into the DOE model, no other similar effort was determined to be adequate for the needs of the electric sector.

A number of maturity models exist. However, the existing array of models is not tailored to address the unique attributes of the electric sector. These include specific functions of the electricity sector as transmission, distribution, and generation; the traditional separation of organizational units; use of control systems and emerging technologies; and the differing requirements of critical infrastructure in comparison with the organizations for which more generic models were developed. Moreover, lack of a consistent evaluation that is specific to the sector prevents insight into the sector-wide cybersecurity capabilities and how they mature over time.

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 collection tool is a multiple choice questionnaire applicable to organizations of different sizes and types throughout the electric sector. There is no undue burden on small businesses or 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.

America's open and technologically complex society includes a wide array of critical infrastructure and key resources that are potential terrorist targets. If the initiative is not executed DOE will not be able to meet the responsibilities under HSPD 7 to make strategic improvements in security which can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. In addition to strategic security enhancements, tactical security improvements can be rapidly implemented to deter, mitigate, or neutralize potential attacks. Not conducting the pilot will restrict the Department’s responsibility to meet the White House request to report on the cybersecurity maturity of the sector. As well, sector partners will have greater difficulty identifying and prioritizing those capabilities and methods needed to protect their systems, and the Nation’s electric grid, from cyber threats.

7. **Explain any special circumstances that require the collection to be conducted in a manner inconsistent with OMB guidelines. (a) requiring respondents to report information to the agency more often than quarterly; (b) requiring respondents to prepare a written response to a collection of information in fewer than 30 days after receipt of it; (c) requiring respondents to submit more than an original and two copies of any document; (d) requiring respondents to retain records, other than health, medical government contract, grant-in-aid, or tax records, for more than three years; (e) in connection with a statistical survey, that is not designed to product valid and reliable results that can be generalized to the universe of study; (f) requiring the use of statistical data classification that has not been**

reviewed and approved by OMB; (g) that includes a pledge of confidentially that is not supported by authority established in stature of 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; (h) requiring respondents to submit proprietary trade secrets, 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.

_

There are none. The package is consistent with OMB guidelines.

8. If applicable, provide a copy and identify the date 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.

This is an emergency request, therefore the Department published a 15-day Federal Register Notice and Request for Comments concerning this collection in the Federal Register on March 30, 2012, volume 77, number 62, and page number 19762. The notice described the collection and invited interested parties to submit comments or recommendations regarding the collection.

The initial draft survey was revised based on responses to comment from an initial utility evaluation. Feedback from this evaluation indicated that a binary scale did not capture meaningful gradations in the implementation of identified practices and the content could be streamlined. As a result, a Likert scale is used for this self evaluation and the survey was restructured from 124 questions to 45 questions with multiple parts.

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

No payment or gift to respondents is being proposed under this information collection.

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

Only anonymous results will be submitted to DOE through industry trade associations. However, DOE will utilize the PCII program's protections to ensure confidentiality and to meet the Department's responsilibity to appropriately protect information associated with carrying out HSPD 7, including handling voluntarily provided information and information that would facilitate terrorist targeting of critical infrastructure and key resources consistent with the Homeland Security Act of 2002 and other applicable legal authorities. DOE is responsible for the final determination with regard to disclosure or nondisclosure of the information and for treating it accordingly under the DOE Freedom of Information regulations at 10 CFR 1004.11.

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 persons from whom the information is requested, and any steps to be taken to obtain their consent.

No questions of a personally sensitive nature, such as sexual behavior and attitudes, religious beliefs included in this information collection. The information collected is related to business processes only.

12. Provide estimates of the hour burden of the collection of information.

The public reporting burden for the collection of information is estimated to average 8 (total burden hours/total annual responses) hours per response. The respondents are voluntary participants completing self-assessments.

The estimate burden of the information collection is as follows:

Total number of unduplicated respondents: 17

Reports filed per person: 1

Total annual responses: The responses are one-time only responses. The estimated total of one-time only responses is 17

Total annual burden hours: 136

Average Burden Per Collection: 8
Per Applicants: 8

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

There is no financial burden for voluntary participants completing self-assessments.

14. Provide estimates of annualized costs to the Federal government.

The cost of the pilot for the Electric Sector Cybersecurity Risk Management Maturity Initiative to the Department of Energy is $175,000.

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

This is a new collection; therefore there are no program changes or adjustments.

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.

The information collected is not intended to be published. No complex analytical techniques will be employed. There will not be a report on the information we collect, other than a report to the White House on the success of the assessment tool and maturity model implementation process. Results will also be communicated to the pilot participants, advisory group members and subject matter experts who contributed to the model development.

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.

DOE is not seeking approval to not 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 Submissions," of OMB Form 83-I.

There are no exceptions to the certification statement.