9110-9P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2014-0015]

National Protection and Programs Directorate;

Notice of completion of notification of Cyber-Dependent Infrastructure And Process for requesting reconsideration of Determinations Of Cyber Criticality. (Authority: E.O. 13636, 78 FR 11737)

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: Public notice of completion of notification and process for requesting reconsideration to owners and operators of cyber-dependent infrastructure.

SUMMARY: The Secretary of Homeland Security has been directed to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In addition to identifying such infrastructure, the Secretary has also been directed to confidentially notify owners and operators of critical infrastructure identified and establish a mechanism through which entities can request reconsideration of that identification, whether inclusion or exclusion from this list. This notice informs owners and operators of critical infrastructure that the confidential notification process is complete and describes the process for requesting reconsideration.

DATES: The agency must receive the reconsideration package before May 15, 2014.

ADDRESSES: Submit reconsideration requests and unclassified written reconsideration materials to CDII@HQ.DHS.GOV. See SUPPLEMENTARY INFORMATION for formatting instructions.

FOR FURTHER INFORMATION CONTACT: The Office of Cyber and Infrastructure Analysis, National Protection and Programs Directorate, United States Department of Homeland Security, Washington, DC 20528, or via e-mail at cdii@hq.dhs.govmailto:carlos.kizzee@dhs.gov.

Responsible DHS Official: Under Secretary, National Protection and Programs Directorate, United States Department of Homeland Security.

SUPPLEMENTARY INFORMATION:

Background: In section 9 of Executive Order (E.O.) 13636 the President directs the Secretary of Homeland Security to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." E.O. 13636, 78 FR 11737 (Feb. 12, 2013). Once that list of infrastructure is transmitted to the President in accordance with sec. 9, the Secretary is further directed to confidentially notify each entity that it has been identified and, "establish a process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications under [this section]." Id at §9(c).

The United States Department of Homeland Security (DHS), in accordance with the consultative process required under E.O. 13636, developed a functions-based approach to identify critical infrastructure where "a cybersecurity incident could reasonably result in catastrophic regional or national effects." DHS consulted with sector stakeholders throughout the identification process including, Sector-Specific Agencies, Sector Coordinating Councils, Government Coordinating Councils, independent

regulatory agencies, subject-matter experts, and critical infrastructure owners and operators.

DHS developed, reviewed, and discussed with private sector entities and trade associations criteria for evaluating when a cybersecurity incident involving critical infrastructure could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. “Catastrophic” was determined to be a higher level of impact than the “debilitating” standard found in the statutory definition of critical infrastructure. The higher threshold ensures that only infrastructure where a cybersecurity incident could cause the greatest impact is identified. The criteria for determining inclusion of the critical infrastructure were designed to assess whether a cybersecurity incident could reasonably result in incapacitation of the infrastructure or function and whether this incapacitation could cause catastrophic regional or national impacts on: Public Health or Safety, Economic Security or National Security.

Identifying cyber-dependent critical infrastructure supports both critical infrastructure needs and national security objectives by (1) providing the Federal government with the ability to more effectively disseminate specific and targeted cybersecurity threat information to identified cyber-dependent critical infrastructure owners and operators; (2) supporting the prioritization, as appropriate, of government resources and programs available to identified cyber-dependent critical infrastructure; and (3) improving government’s understanding of the systems or assets whose incapacity or disruption would have catastrophic consequences in furtherance of government planning, protection, mitigation and response efforts to be provided in partnership with

impacted state, local, territorial, tribal and private sector entities in the event of a cyber incident.

The Secretary presented the initial list of identified infrastructure to the President, through the Assistant to President for Homeland Security and Counterterrorism on July 19, 2013. In accordance with E.O. 13636, this list will be reviewed and updated annually.

DHS has completed the process of notifying owners and operators of critical infrastructure that were included on the July 19, 2013 initial list. If critical infrastructure owners and operators have not been contacted by DHS in connection with their status on the initial list, then such infrastructure has not been included on the initial list. Such infrastructure may be included in subsequent updates based on the outcome of reconsideration requests, annual reviews, or amendments to the list.

The opportunity for reconsideration of initial identifications by DHS is available to all critical infrastructure owners and operators, whether or not their infrastructure has been identified as cyber-dependent by DHS, in accordance with this notice. The opportunity for reconsideration will be provided annually.

The Secretary has delegated to the Under Secretary for National Protection and Programs the authority to address reconsideration requests and to make determinations in connection in subsequent updates.

Definitions

"Critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets

would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

"Cyber dependent" means critical infrastructure that utilizes computers, electronic communications systems, electronic communications services, wire communication, and/or electronic communication, including information contained therein, in order function or be maintained.

"Cyber incident" means an event or series of events that impairs the confidentiality, integrity, or availability of electronic information, information systems, services, or networks.

"Reconsideration official" means the Under Secretary for National Protection and Programs, or her or his designee, who will consider requests for reconsideration in accordance with the process set forth in this notice.

Impact of being identified under sec. 9

The primary purpose of identifying critical infrastructure under sec. 9 of E.O. 13636 is to better understand national and regional cyber dependencies and consequences across critical infrastructure, inform planning and program development for federal critical infrastructure security and resilience programs, and enable improved cyber risk management by the identified critical infrastructure owners and operators. Owners and operators of identified cyber-dependent critical infrastructure have the opportunity to request expedited processing through the DHS Private Sector Clearance Program, which may provide access to classified government cybersecurity threat information as appropriate. Cyber-dependent critical infrastructure may also be prioritized for routine and incident-driven cyber technical assistance activities offered by DHS and other

agencies. Additionally, owners and operators of identified cyber-dependent critical infrastructure are encouraged to participate in the National Institute of Standards and Technology (NIST) cybersecurity framework for critical infrastructure ("NIST framework"). As Federal government resources and programs develop and improve to enhance the security and resilience of critical infrastructure against cybersecurity threats, cyber-dependent critical infrastructure will be a continued priority.

Reconsideration Process

Submitting a reconsideration request

Reconsideration of identifications under sec. 9 of E.O. 13636 will be based on an evaluation of new information provided to DHS by the requesting entity. An entity must initiate the reconsideration process in writing. However, the entity also may request a meeting with a DHS official (in person or by phone) to discuss the additional information they will provide in support of their reconsideration request or to seek additional information about the basis for identifications. DHS will consider meeting requests on a case by case basis and identify an appropriate official to participate in such meetings on behalf of the reconsideration official.

Owners and operators of critical infrastructure entities or their authorized agents may initiate a reconsideration request by sending an email to CDII@HQ.DHS.GOV including:

1. the entity for reconsideration;

2. the name, title, telephone number and email address of a designated point of contact, whether an employee or non-employee agent, for the owner or operator of that

entity to whom all communications related to the reconsideration process will be directed; and

3. if desired, a request for a meeting with DHS representatives.

DHS will confirm the submission of each reconsideration request with an email to the submitting entity and will provide a reconsideration request number within three days of receipt. Where the requesting entity has requested a telephonic or in-person meeting, a representative of DHS will contact the entity at the email address provided in the initial request to schedule a meeting or inform the entity that the requested meeting is not available.

Submission of Reconsideration Materials

Following DHS confirmation of the request, entities may submit reconsideration materials as part of an in-person or telephone meeting or in writing. Entities who submit written documentation in lieu of a meeting or who choose to provide additional documentation following a meeting should submit the information via email (with exceptions noted below) in the form of a single attachment. All pages submitted to DHS should be double-spaced 12 point Times New Roman text or visual material, with 1" margins and page numbers. Supporting documentation should be organized and labeled. Entities should include the DHS-provided reconsideration request number on each page of the submission.

Documentation used to justify a change in status for an entity with respect to identified cyber-dependent critical infrastructure may constitute protected critical infrastructure information (PCII) if it satisfies, and is submitted in accordance with, applicable requirements. The PCII program is an information-protection program that

enhances voluntary information sharing between infrastructure owners and operators and the government. In order to ensure handling under the provisions of the PCII program, owner operators must submit information consistent with the Critical Infrastructure Information Act (6 U.S.C. 131 *et seq*), the PCII final rule (6 CFR part 29), and the PCII Program Manual. Additional information regarding the PCII program may be found at http://www.dhs.gov/pcii.

Classified information must not be transmitted to mailto:cdii@hq.dhs.gov; however, a request for guidance on alternate submission guidance may be sent, without any classified information, to cdii@hq.dhs.gov. DHS may in its sole discretion grant a reasonable extension to the reconsideration submission for the purpose of accommodating a request to submit classified information.

Reconsideration request review

A preliminary review by DHS following a meeting or submission of the reconsideration materials will evaluate whether any additional information is needed to make a decision on the reconsideration request. DHS will contact the submitter within 30 days of the meeting or submission to request additional information, if needed, or to confirm that the reconsideration package is complete. If additional information is requested, the submitter will have up to 60 days from the date of DHS's request to provide such information, and DHS will have another 30 days from the additional submission to deem the package complete. Following receipt and review of a complete reconsideration package, DHS will provide requesting entities with a written response including the basis for its determination.

If a complete reconsideration package is not received by DHS before May 15, 2014, any information provided by a submitter may be considered in connection with the next annual update rather than as a request for reconsideration of this year's determination.

In considering requests for reconsideration, DHS may consult with sector specific agencies and other appropriate federal entities. Information submitted to DHS, including appropriately submitted PCII, will be protected in accordance with applicable requirements and used only for permitted purposes.

Entities may contact cdii@hq.dhs.gov at any time to request a status update during the reconsideration request review process. After a determination has been made in connection with the request, subsequent reconsideration requests will not be accepted until the next annual review.

Dated: April 11, 2014.

Suzanne Spaulding,

Under Secretary,

National Protection and Programs Directorate,

Department of Homeland Security.

[FR Doc. 2014-08702 Filed 04/16/2014 at 8:45 am; Publication Date: 04/17/2014]