9110-9P

DEPARTMENT OF HOMELAND SECURITY

National Protection and Programs Directorate

[Docket No. DHS-2015-0068]

National Protection and Programs Directorate Seeks Comments on Cyber Incident Data Repository White Papers

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: Notice.

SUMMARY: The Department of Homeland Security's (DHS's) National Protection and Programs Directorate (NPPD) announces that it is seeking comments on three white papers prepared by NPPD staff from any interested party, including, but not limited to: members of the cybersecurity and insurance communities; chief information security officers (CISOs); chief security officers (CSOs); academia; Federal, State, and local governments; industry; and professional organizations/societies. Links to the white papers are posted on the cybersecurity insurance section of DHS.gov: http://www.dhs.gov/publication/cyber-incident-data-and-analysis-working-group-white-papers. Comments will assist NPPD further refine the content of the white papers to address the critical need for information sharing as a means to create a more robust cybersecurity insurance marketplace and improve enterprise cyber hygiene practices across the public and private sectors.

DATES: The suggested dates for submission of comments on the white papers are: March 24, 2016 through May 24, 2016.

ADDRESSES: Comments on the white papers must be submitted to NPPD via email to the following address: cyber.security.insurance@hq.dhs.gov.

FOR FURTHER INFORMATION CONTACT: Matt Shabat, Director, Performance Management, Office of Cybersecurity and Communications at 703-235-5338 or by e-mail at Matthew.Shabat@hq.dhs.gov.

SUPPLEMENTARY INFORMATION:

Background: Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: 1) promoting the adoption of preventative measures in return for more coverage; and 2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection. Many companies forego available policies; however, citing as rationales the perceived high cost of those policies, confusion about what they cover, and uncertainty that their organizations will suffer a cyber attack. In recent years, NPPD has engaged key stakeholders to address this emerging cyber risk area.

Between October 2012 and April 2014, DHS NPPD conducted several workshops, which brought together a diverse group of private and public sector stakeholders – including insurers, risk managers, CISOs, critical infrastructure owners, and social scientists. Workshop participants examined the current state of the cybersecurity insurance market and how to best advance its capacity to incentivize better cyber risk management.

During those workshops, participants expressed strong support for the creation of a trusted cyber incident data repository. As envisioned, the repository would store, aggregate, and analyze cyber incident data relevant to the cyber risk management community, including risk mitigation experts (CISOs, CSOs, cybersecurity solutions providers); risk transfer experts (insurers); and other cybersecurity subject matter experts (the academic and scientific communities). As further envisioned, DHS or other Federal departments or agencies would not build or manage such a repository. A resulting repository could potentially be managed by a private organization.

In February 2015, as a follow-on to the workshops, NPPD established a Cyber Incident Data and Analysis Working Group (CIDAWG), comprised of CISOs and CSOs from various critical infrastructure sectors, insurers, and other cybersecurity professionals. The CIDAWG is currently exploring how anonymous cyber incident data sharing could help grow the cybersecurity insurance marketplace through a legally compliant, privacy respecting, and trusted cyber incident data repository and repository data supported analyses. In turn, this would work to improve cybersecurity for U.S. public sector agencies and private sector companies. To accomplish this, the CIDAWG has worked to develop key findings about:

1. The value proposition of a cyber incident data repository;

2. The cyber incident data points that should be shared into a repository to support needed analysis;

3. Overcoming perceived obstacles to sharing into a Cyber Incident data Repository; and

4. A potential repository's structure and functions.

The findings of this effort to date are summarized in a series of three white papers.

This announcement explains the process for submitting comments on the white papers. Comments on the white papers are valued and will enable NPPD to incorporate input from a wide audience. Each white paper is briefly detailed below, followed by questions on which NPPD seeks comments.

1) The Value Proposition. Details how a cyber incident data repository could help advance the cause of cyber risk management and, with the right repository data, the kinds of analysis that would be useful to CISOs, CSOs, insurers, and other cybersecurity professionals. NPPD seeks comments on the following:

    a. What value would an anonymized and trusted cyber incident data repository, as described in the white paper, have in terms of informing and improving cyber risk management practices?

    b. Do you agree with the potential benefits of an anonymized and trusted repository, as outlined in the white paper, that enterprise risk owners and insurers could use to share, store, aggregate, and analyze sensitive cyber incident data?

    c. Are there additional benefits of an anonymized and trusted repository that are not mentioned in the white paper? Please explain them briefly.

d. What kinds of analysis from an anonymized and trusted repository would be most useful to your organization?

2) Cyber Incident Data Points and Repository-Supported Analysis. Addresses the kinds of prioritized data categories and associated data points that should be shared among repository users to promote new kinds of needed cyber risk analysis. NPPD seeks comments on the following:

a. Could specific data points within the 16 data categories effectively inform analysis to bolster cyber risk management activities?

b. Are the 16 data categories accurately defined?

c. What additional data categories could inform useful analysis to improve cyber risk management practices?

d. What do these additional data categories mean from a CISO or other cybersecurity professional perspective?

e. Please rank the level of importance for each data category, including any additional data categories that you have identified.

f. What value does each data category and associated data points bring to a better understanding of cyber incidents and their impacts?

g. What does each data point actually mean (and to whom); and which ones are the greatest priority, to which stakeholders, and why?

h. How easy/difficult would it be to access data associated with these categories in your organization and then share it into a repository and why?

3) Overcoming perceived obstacles to sharing into a Cyber Incident data Repository. Identifies perceived obstacles to voluntary cyber incident data sharing and offers potential approaches to overcoming those obstacles. NPPD seeks comments on the following:

a. Would your organization be interested in contributing to a cyber incident data repository and using repository-supported analysis to improve your organization's risk management practices?

b. What obstacles do you anticipate – both internal and external to your organization – that might prevent the sharing of cyber incident data into a repository?

i. Who might say 'no' to sharing and why?

c. What mechanisms, policies, and procedures could help overcome these obstacles to sharing?

In this call for comments on the white papers, NPPD is seeking input on any or all of the above listed questions. NPPD may use comments to further develop the content of each white paper as appropriate. Do not include ideas for specific proposals in your comments on the white papers (i.e., do not discuss your specific solution to the repository concept). This solicitation for comments on white papers is neither a Request for Proposals (RFPs) nor should it be viewed as a request for pre-proposals. Rather, it is a way to include ideas from the public to enhance the research and findings of the CIDAWG to better understand the potential of an anonymized and trusted cyber incident data repository to address the cybersecurity needs of the public and private sectors.

Comments on white papers must not contain proprietary information. Submission of comments on any of the white papers means that the author(s) agrees that all the information in the comments on the white papers can be made available to the public. Information contained in these comments on the white papers will be considered and combined with information from other resources, including NPPD, the CIDAWG, other government agencies, cybersecurity and insurance communities, and other stakeholders to refine the focus of the white papers and are part of NPPD’s collaborative outreach. Comments on the white papers are a valuable resource that adds to NPPD’s understanding of the significance and scope of national cybersecurity and critical infrastructure needs. NPPD’s statutory authority is the Critical Infrastructure Partnership Advisory Council, which is consistent with sec. 201 of the Homeland Security Act of 2002 (the "Act"), 6 USC 121, and pursuant to sec. 871(a) of the Act, 6 USC 451(a).

Dated: March 16, 2016

Matthew Shabat
Director, Performance Management
Office of Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

[FR Doc. 2016-06856 Filed: 3/25/2016 8:45 am; Publication Date: 3/28/2016]