OMB Control No. – 0693-0043 – NIST Generic Clearance for Usability Data Collections

Cyber Supply Chain Risk Assessment

FOUR STANDARD SURVEY QUESTIONS

1. Explain who will be surveyed and why the group is appropriate to survey.

The entities to be surveyed are commercial firms who have an interest and need in ensuring effective cybersecurity is in place to mitigate against cybersecurity threats. The questions are focused on assessing the cybersecurity practices of these firms.

While the vast majority of companies have a business need to minimize cybersecurity risk, given the voluminous number of commercial entities that exist, it is not feasible to sample the entire universe of commercial firms. As such, this survey is focused on vendors who either desire to enter into or have an existing contractual relationship with either (or both) the Federal Government or a cybersecurity insurance provider. Both the Government and the Insurance sector are interested in promoting the adoption of effective cybersecurity practices and being able to better assess and manage supplier-related cybersecurity risk exposure.

2. Explain how the survey was developed including consultation with interested parties, pre-testing, and responses to suggestions for improvement.

The survey was developed in iterations through a collaborative effort by officials from experts from the University of Maryland's (UMD's) Robert H. Smith School of Business' Supply Chain Management Center, NIST, GSA, Zurich Insurance Group, and Beecher Carlson Insurance Services.

By collaborating with the insurance industry, the government is able to align its cybersecurity supply chain risk management activities directly with the criteria used by the insurance industry for underwriting cybersecurity insurance policies. The synergies created by bringing together the power of Federal purchasing and the analytical methodologies used for insurance underwriting are anticipated to have a significant positive effect on the adoption of the resulting, consensus-based risk management practices, across the Federal supply chain and throughout the broader economy.

The survey leverages the Framework for Improving Critical Infrastructure Cybersecurity (developed under Executive Order 13636) and NIST's Supply Chain Risk Management Practices for Federal Information Systems and Organizations (NIST Special Publication 800-161). Both of these documents have been embedded in the "Cyber Risk Portal Assessment Tool Set" developed by UMD over the course of a five-year series of grants from NIST.

The survey questions are based upon and organized in a manner that aligns with the categories and subcategories of the Cybersecurity Framework, which is being widely adopted across many industry segments. The Framework is voluntary and was created through collaboration between industry and government, and consists of standards, guidelines, and practices to promote cyber protection. It provides for a prioritized, flexible, repeatable, and cost-effective approach to help organizations manage cybersecurity-related risk.

3. Explain how the survey will be conducted, how customers will be sampled if fewer than all customers will be surveyed, expected response rate, and actions your agency plans to take to improve the response rate.

The survey is voluntary in nature and is intended to be completed by commercial suppliers of goods and/or services. Targeted outreach will occur to approximately 15,000 commercial entities, via an email campaign to vendors who provide information and communications technology good and services, such as those that have GSA IT 70 Schedule contracts, firms that have or may be interested in purchasing cybersecurity insurance, and private sector companies that have indicated interest in adopting the cybersecurity framework to improve their cybersecurity posture. In many instances, a vendor may fall into more than one of these above categories.

A minimum of 250 responses is required to be able to conduct the research and perform the required statistical analysis. There is no upper level threshold. It is expected that the response rate will meet or exceed 750 responses and the response time is estimated to be 90 minutes per response.

Volunteer participants are instructed in the email they receive to register at https://cyberchain.rhsmith.umd.edu to access the secure "CyberChain" online portal. The University of Maryland is providing a virtual help desk for registration and survey support. This portal webpage also provides video content users can access to learn more information about cyber supply chain risk. Closed captioning is available for the videos.

Registrants will have approximately 45 days to complete the survey. The survey will open on January 30, 2017 and the last day to complete the survey will be March 15, 2017. The portal provides visualization indicators of which portions of the questionnaire has been completed and how many questions remain. Three reminder notices will be sent out to registrants that have not yet completed their survey (February 7, 2017, February 14, 2017, and March 1, 2017). Copies of the initial email and the there reminder emails are provided as an attachment.

The survey has also been designed to provide direct and immediate benefit to the surveyed organization.   Once the questionnaire is completed, the respondent will have access to a printable, dashboard-type visual depiction of the company's assessment results indicating to what extent they have implemented the Framework (partial, risk-informed, repeatable, or adaptive) At a glance, a company will be able to see where they have opportunities to enhance their cybersecurity practices.

4. Describe how the results of the survey will be analyzed and used to generalize the

results to the entire customer population.

The survey results provide for a baseline set of research data about the cybersecurity “performance profile” of entities (contractor/subcontractor/supplier) to be analyzed for the purpose of identifying statistically valid causal linkages between a set of cybersecurity risk indicators to a level of entity performance. No such data-driven validation of material connections between cybersecurity risk indicators and performance levels exists today.

Completed surveys are “anonymized” and neither GSA nor NIST will be privy to any individual company responses nor have knowledge about the identities of the firms that responded.

Cyber breaches are an indicator of cybersecurity risk. Cyber breach data, obtained by UMD via a third party data subscription as well as obtained from public sources such as the SEC, will be collected for a minimum of six months, following the completion of the performance profile surveys. The names of companies that have experienced a breach will not be disclosed to either GSA nor NIST. When there is a match between a company that has experienced a breach and has also completed the survey, UMD will “map” that data to that same company’s performance profile. Statistical data analysis methods will be used to determine whether there may be, and to what level of statistical significance, any causal relationships between a discrete or a set of cybersecurity practices and the likelihood that a cyber breach may occur or be prevented.

A similar research and analysis methodology was used to determine causal relationships between compliance practices and safety-related incidents in the motor carrier industry.

The results of the research and analysis will be output into a formal report of findings, describing findings about the significance of relationships between assessed cybersecurity performance practices and cybersecurity performance outcomes.