OMB CONTROL NUMBER 0693-0043
NIST GENERIC CLEARANCE FOR USABILITY DATA COLLECTIONS

NIST, Information Technology Laboratory (ITL)
Cyber-Supply Chain Risk Management Best Practices Interview

Survey Questionnaires for: Questions for industry personnel about their cyber-supply chain risk management practices

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

As part of an in-depth interview study of cyber supply chain risk management best practices, the Computer Security Division, of the Information Technology Laboratory (ITL), of the National Institute of Standards and Technology (NIST) intends to recruit 30 participants. Participants will be individuals who have first-hand experience in supply chain risk management. Participants will be recruited via phone call or email from recommendations from NIST personnel.

The purpose of this project is to understand industry best practices for cyber-supply chain risk management, as well as challenges they face in order to inform new technology development and standardization. The project will investigate organizations' experience by understanding:

- The cyber-supply chain risk management process from the perspectives of supply chain managers, quality control specialists, and third-party risk managers.
- Cyber supply-chain risk management technology usage, including medium/form/modality
- Industry organizations' views on cyber-supply chain risk management technology (current and future looking)
- Challenges and limitations for evaluating and managing cyber-supply chain risk

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

The interview questions were developed and refined based on discussions with Supply Chain Risk Management subject matter experts at NIST and Boston Consulting Group (BCG) Platinion.

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.

Cyber-supply chain risk management is still an emerging discipline but is closely related to well-defined areas of quality control, third-party risk management, and similar disciplines. Several industries have built solutions to cyber-supply chain risks independently, often using their own language and terms, but implementing very similar practices. NIST will attempt to identify up to 10 organizations to interview from the

following industries:

- Automotive
- Chemical
- Defense/Aerospace
- Electronics
- Energy
- Entertainment
- Food
- Medical Devices
- Pharmaceutical
- Retail
- Software
- Telecom
- Textile

For each organization, we anticipate that one person may not be able to answer all questions, thus **up to three people may participate from each organization**, for a total of 30 participants. More than one person from each organization may participate in a single interview. Each interview is expected to take 60 minutes.

Participants will be identified based on recommendations from NIST and BCG Platinion subject matter experts. Once an individual agrees to participate, an interview appointment will be scheduled virtually at a particular time agreed upon by both the participant and researchers. The data will be collected through semi-structured interviews. The interview includes 27 questions may be covered over the two interviews per organization, for a total of 60 minutes. The interview will not be recorded, but notes of responses received will be transcribed.

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

We intend to work with the organizations to write a case study on their organizations' cyber supply chain risk management best practices. The organization will be given the opportunity to approve, edit, anonymize, or reject the case study for publication. In addition, NIST will use the qualitative data analysis technique of grounded theory to create a list of cyber-supply chain risk management best practices and opportunities for research and development. We will compare the qualitative responses across different types of industry organizations. These results will be used along with other research to inform a list of commonly applicable best practices.

There will be no collection, storage, access, use, or dissemination of personally identifiable information from the interviews except for contact information if the organization requests such information be included in the case studies. Data will be linked to an organization, but not to a specific respondent.