OMB Control #0693-0043
Expiration Date: 09/30/2025

Cybersecurity Supply Chain Survey Tool

FOUR STANDARD SURVEY QUESTIONS

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

The Information Technology Laboratory's Computer Science Division of the National Institute of Standards and Technology (NIST), a non-regulatory agency of the Department of Commerce (DOC), proposes to conduct data collection under this generic data collection on cybersecurity supply chain risk management.

Managing the cybersecurity of the supply chain continues to be an evolving challenge for organizations in both private and public sectors. The Cybersecurity Supply Chain Survey Tool is a combined survey questionnaire and knowledge resource to provide insights for public and private organizations to evaluate and manage their strategies and processes to minimize cybersecurity supply chain risks. It offers a series of questions for the participants to address in a trusted and anonymized environment and, based on the entered responses, provides the analysis, and directs users to relevant guidance and standards for further research. The data collected will provide insights into organizations' current practices in managing their cybersecurity risks and help provide feedback to improve the survey.

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

The original version, the cyber supply chain assessment tool, was developed jointly with the University of Maryland College Park, R.H. Smith School of Business (UMD), as part of the research under a NIST grant and GSA sponsorship [1]. The tool is composed of a survey questionnaire developed with the knowledge gained from decade-long research involving a process of regional field studies with industry over a several-year period and statistical analysis of the effect on an organization's breach profile based on the extent of its adoption of policies and practices as defined within the Cybersecurity Framework (CSF) [2].

The current iteration, the cyber supply chain survey tool, is cloud-based with a web interface for participants to enter the survey data anonymously and securely. The survey questions ask for information on various organizations and cyber supply chain-related practices. The questions are grouped according to the NIST's five cybersecurity framework functions (Identify, Protect, Detect, Respond, Recover). The tool provides a score by categories within each CSF function from the participants' entered data.

Data collected by NIST researchers will be used to provide feedback to improve the questionnaire and help plan the direction of future research. The information collected will not be directly disseminated to the public, but aspects or portions of the information collected may be used to support research published in various journals and conferences.

One of the consistent feedback items from past participants is the need for a trusted and anonymous environment. To build confidence that there will be no attribution to individuals or organizations in the analyzed data, the application includes capabilities to protect and encrypt the data in transit and at rest. The application does not require users to log in or track their IP address or cookies to avoid collecting personally identifiable information (PII) and minimize entry traceback. The NIST Research Protection Office has determined that the application is not human subjects research as defined in 15 CFR 27.

The application deployment is conducted in phases, where internal and external testers and evaluators can provide feedback. Phase 1 uses test data, and the audience is a limited set of federal partners. Phase 2a's audience is limited to the general federal civilian agencies using test data for more review and feedback. Phase 2b's audience continues to be limited to the federal civilian agencies but no longer using test data. When the tool has been tuned through the federal usage and PRA issues are sufficiently addressed, phase 3 will be initiated.

This information collection and dissemination complies with the NIST Chief Information Officer (CIO) Information Quality Guidelines and Standards. Quality will be ensured and established at levels appropriate to the nature and timeliness of the information to be disseminated. It will also include all pre-dissemination reviews, as the Information Quality Guidelines and Standards require.

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

To reduce the burden on NIST's customers, the online data collection function is a survey with a series of questions. The answers to the questions primarily use simple yes/no and Likert scale selection. The survey questions are mapped to the Cybersecurity Framework categories. NIST's Online Information Reference directs the participant to the relevant sections of the guidance and standards for further exploration.

Once data has been gathered, the survey takes about 40 minutes to complete. Based on previous surveys, the expected response rate is approximately 200 organizations.
Total burden is calculated at 200 respondents * 40 minutes / 60 = 133 burden hours

No PII is collected in this instrument.

There will be a combination of outreach efforts to improve the response rate, including announcements, directed emails, and presentations to the interested communities.

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

Data collected by NIST researchers will be used to provide feedback to improve the questionnaire and help plan the direction of future research in cybersecurity risk analytics and measurement. Selected areas of cybersecurity have better defined, broadly accepted and widely used quantitative measurements and metrics (e.g., mean time to detect and mean time to respond for incident response; tracking number of detected vulnerabilities and time to complete patching in vulnerability management; measuring phishing click rates, awareness training completion rates in security awareness), quantifying overall cybersecurity risk continues to be challenging. Information gathered from this survey can inform NIST research to both identify areas that could benefit from additional technical guidelines to quantify risk, and an methodology for risk aggregation and communication.

The information collected will not be directly disseminated to the public, but aspects or portions of the information collected may be used to support research published in various journals and conferences.

References

[1] University of Maryland College Park, R.H. Smith School of Business (2017). The Cyber Risk Predictive Analytics Project. Available at https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/UMD%20Final%20Report-Cyber%20Risk%20Analytics%20Project%20revised%20tc%20november%2025%202017.pdf

[2] Boyson S, Corsi TM, Paraskevas JP (2022). Defending digital supply chains: Evidence from a decade-long research program. *Technovation* 118. https://doi.org/10.1016/j.technovation.2021.102380