Good [morning/afternoon] [Chief/or other title],

The National Institute of Standards and Technology (NIST) is conducting a limited number of interviews to develop case studies and inform guidance on effective practices for cyber supply chain risk management.

Your participation in this effort will be greatly appreciated and will help advance the state of cyber supply chain risk management by improving awareness of effective practices as they exist "in the wild".

Background

Cyber supply chain risk management (C-SCRM) involves identifying, assessing, and mitigating supply chain risks for information and operational technologies. It includes mitigating risks such as counterfeits, third party cybersecurity risk, poor quality, and other risks.

This work is a continuation of past research available here: https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/Best-Practices

Interviews

As part of our research, we are conducting interviews of a broad range of organizations to help determine a baseline of effective practices currently used. The interviews will be conducted by phone and last approximately one hour each. Since one person within an organization may not be able to answer all of the interview questions, more than one professional in the organization may participate and the interview may be broken up into two separate interviews for a total of 60 minutes. The interviews will follow a template of questions that will be shared with the interviewee prior to the appointment.

The interviews themselves are confidential. The interviews will not be recorded, but notes will be transcribed. At any time during the interviews, the interviewees may request that a statement not be transcribed or used.

Benefits of Participation:

For each organization that participates in the interview(s), a case study will be written that highlights those practices which the organization has found most valuable. The organization will be given the opportunity review, edit, and approve for distribution their case study.

The case studies will be attributed to the organization, unless the organization requests the case study be anonymized, in which case the organization will be identified by their industry sector (e.g. "small utility company"). No individuals will be identified or named unless the organization requests this information be published as part of the case study (e.g. contact information).

In addition, the information garnered from the interviews – including information not published in the case studies - will be used to inform publications listing practices for cyber supply chain risk management and to inform future research efforts. In no instance will information from the interviews not approved by the organization for public distribution be attributed to the organization or any individual.