



MANAGING SUPPLY CHAIN RISK THROUGH COMMERCIAL STANDARDS

JOANNE WOYTEK,
NASA SEWP PROGRAM DIRECTOR



The topic of standardizing the approach to supply chain risk management has recently emerged as a hot topic for both government and industry. For NASA SEWP (Solutions for Enterprise-Wide Procurement) this is a continuation of a long-standing commitment to support, understanding and dissemination of acquisition and supply chain concerns. SEWP has been a member of The Open Groupⁱ since its inception in 1996 and currently serve on their governing board.ⁱⁱ The Open Group is an international standards body, and in 2013 created the first commercial standards for supply-chain risk management in ISO/IEC 20243-1:2018 Information technology — Open Trusted Technology Provider™ Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products.ⁱⁱⁱ

***Congratulations to NASA's own,
Karla Smith-Jackson, for emceeding
this year's World Congress!***



In December 2020, the Government Accountability Office (GAO) released a report, "Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks".^{iv} The report states that agencies are required to "develop organizational ICT SCRM requirements for suppliers" and "develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment."

Supply Chain Risk Management (SCRM) pertaining to technology and government operations has emerged quickly as a matter of critical national and geo-political importance.



Confusion over what to do, by whom, and for what purposes is still being made clear, as agency leaders, mission and business owners, and system owners look for ways to help shore up what is needed within their practices.

To help bring clarity to a complicated topic, the program initiated and sponsored a study^v to compare how closely the commercial standards mapped to the NIST recommendations for SCRM, looking primarily at NIST 800-161 and NITST IR 7622.

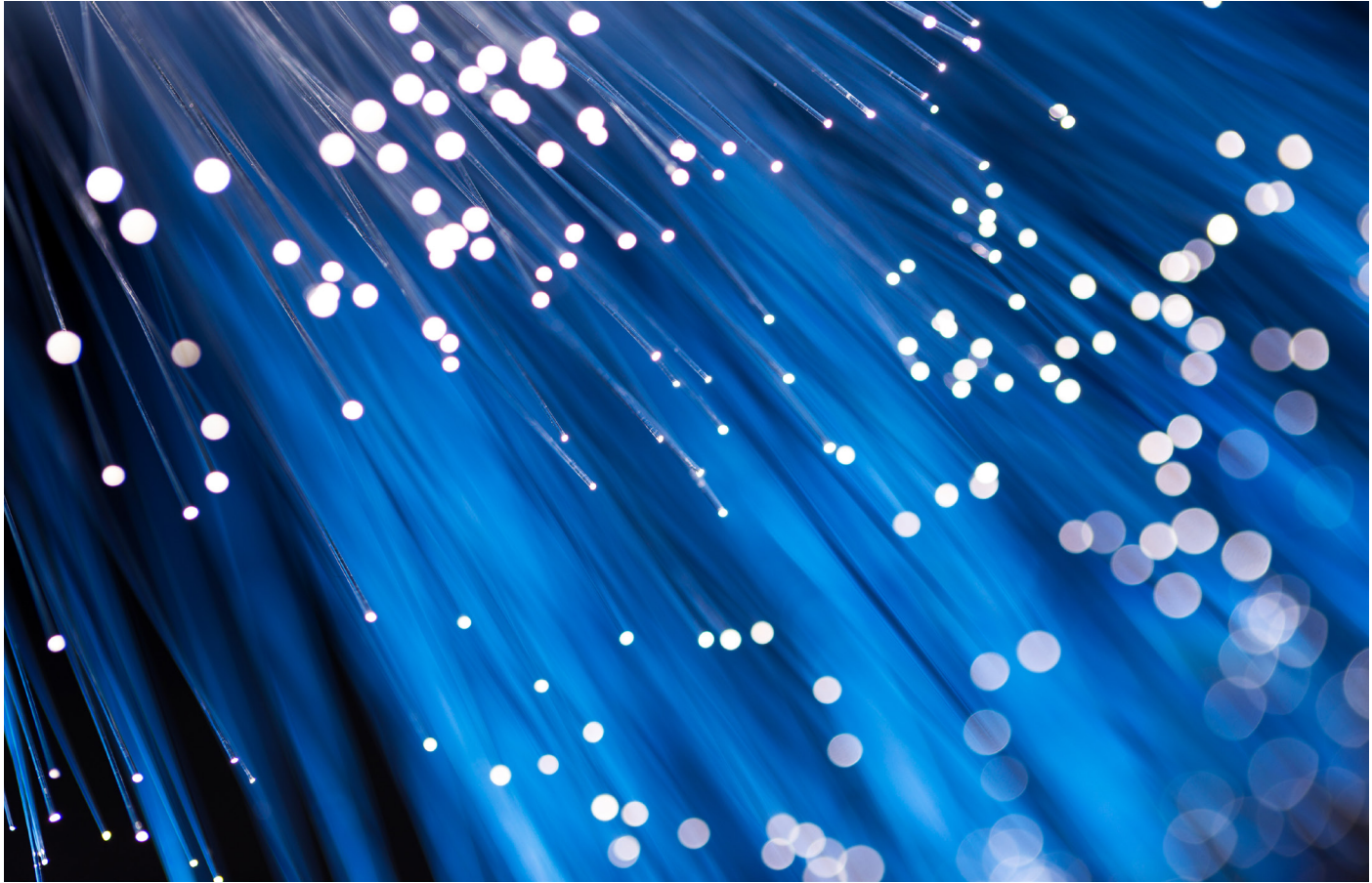
This was a critical step towards clarity, as OMB Circular NO.A-119 states, “All federal agencies must use voluntary consensus standards in lieu of government-unique standards in their procurement and regulatory activities, except where inconsistent with law or otherwise impractical.”^{vi}

The federal government has been taking direct actions to help secure their Information and Communication Technology (ICT) and Audio Visual (AV) assets that enter the government’s federal infrastructure. Because digital assets and information are relied upon by everyone in our nation, efforts are underway to require vendors, who serve the federal government, to increase their efforts in securing the assets that are contained and transferred within our infrastructure.

There has been abundant confusion as this topic has emerged, since it appears to blend traditional supply chain management practices with cyber-hygiene elements into a single approach.

Further, NIST already concluded that “there are a surprising number of standards and guidelines for supply chain risk management” as they have identified ISO 20243 for acceptable use for help with protecting the Cyber Supply Chain.^{vii} This study brought specificity as to how agencies can leverage the ISO standards.

The NASA SEWP program has embedded SCRM practices into our program as a way to help mitigate supply chain risks. These practices are baked into our program and platform. In my next article, I will go into more detail into how data plays a critical role in this endeavor.



- i* <https://www.opengroup.org/>
- ii* <https://www.opengroup.org/governing-board>
- iii* <https://www.iso.org/standard/74399.html>
- iv* Government Accountability Office. (2020). Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks. (GAO Publication No. 21-171). Washington, D.C.: <https://www.gao.gov/assets/gao-21171.pdf>
- v* https://www.sewp.nasa.gov/documents/OTTPS-NIST_CrossWalk_NASA_SEWP.pdf
- vi* United States. Office of Management and Budget. OMB Circular NO.A-119. Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities. [Washington, D.C.]: Executive Office of the President, Office of Management and Budget.
- vii* National Institute of Standards and Technology. Best Practices in Cyber Supply Chain Risk Management Conference Materials. Cyber Supply Chain Standards Mapping and Roadmap. <https://csrc.nist.gov/CSRC/media/Projects/SupplyChain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Standards-Mapping.pdf>

PROMOTIONAL CONTENT