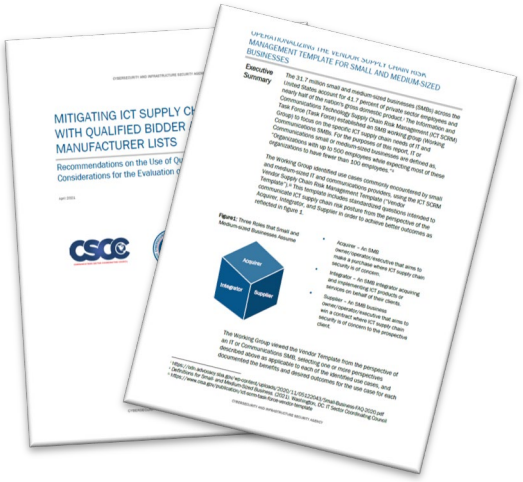
IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

MITIGATING ICT SUPPLY CHAIN RISKS WITH QUALIFIED BIDDER AND MANUFACTURER LISTS

OVERVIEW



The world is becoming more dependent on, and more connected by, information and communications technology (ICT) products and services. At the same time, the global ICT supply chain continues to increase in sophistication and complexity. Hundreds of entities in multiple countries may contribute to a single product, including mining rare earth metals, developing integrated circuits or software, performing the final assembly of the product, or storing and delivering finished goods or repaired parts. Each of these entities and their associated supply chain partners can contribute to overall supply chain risk.

The Cybersecurity and Infrastructure Security Agency (CISA) ICT Supply Chain Risk Management (SCRM) Task Force's report, Mitigating ICT Supply Chain Risks with Qualified Bidder (QBL) and Manufacturer Lists (QML), provides realistic, actionable, economically feasible, and risk-based recommendations surrounding the use of "Qualified Lists" as one tool among many, that can help organizations better manage ICT supply chain risk.

ACTIONABLE GUIDANCE FOR PUBLIC AND PRIVATE ORGANIZATIONS

This report explains the purpose and benefits of Qualified Lists, provides a description of factors that inform a decision to build/rely on a QBL/QML for ICT products and services, and proposes actionable recommendations for incorporating SCRM considerations into new and existing ICT-related qualified list criteria and program processes. These recommendations are intended to be relevant and informative for both public and private sector purchasers and providers of ICT products and services.

As defined by the Federal Acquisition Regulation, and for the purpose of the report, a QBL is a list of bidders who have had their products examined and tested and who have satisfied all applicable qualification requirements for that product or have otherwise satisfied all applicable requirements. A QML is a list of manufacturers who have had their products examined and tested and who have satisfied all applicable qualification requirements for that product.

Establishing and utilizing vetted, qualified sources of supplies can reduce an organization's exposure to security, integrity, resilience, or quality risks. Incorporating cyber supply chain risk management qualification criteria into existing or new qualification list processes can provide a targeted and effective means for providing assurance that an ICT supplier and their product or service is sufficiently trustworthy. Table 1 provides a summary of the benefits, costs, and risks associated with QLs.

Table 1: Summary of Benefits, Costs, and Risk Associated with Qualified Lists (QL)

Benefits	Costs and Risks
▪ Provides for a means to readily identify which entity(ies), product(s), or service(s) have been shown by an organization to satisfy a set of criteria, saving time and resources that would otherwise be spent evaluating against those criteria on a project-by-project basis. Promotes the use of standards. ▪ Greater assurance that experienced, qualified personnel perform assessments, and do so in a consistent and fair manner.	▪ Requires significant investment of resources (time, money, expertise) to build and maintain. ▪ Criteria must be tailored carefully to the security and functional objectives of those relying on the list or it may lead to unintentional assumption of risk. Lack of clarity and understanding regarding the objective of the list and criteria considered can engender a false sense of security among list users.

▪ Qualification requirements and processes allow for more of a life cycle focus vs. point in time. ▪ Transparency about qualification is enabled by ensuring there is documentation about, and access to the QL, and information about QL purpose, requirements, process steps, timeframes, and qualification-associated costs. ▪ Enables a more streamlined or accelerated procurement process. Concentrates and optimizes the use of resources involved in conducting an assessment. ▪ Allows for a means to selectively raise the bar vs. taking a one-size-fits-all approach (e.g., QL for Continuous Diagnostics and Mitigation tool providers vs. applying same criteria and evidentiary requirements for all ICT tool providers). ▪ Reduction in burden to industry by reducing need to respond to duplicative, and potentially conflicting, requirements.	▪ Failure to build and manage lists appropriately can expose those relying on the list to security vulnerabilities, lack of availability or logistical capability, legal liability, or other risks. ▪ Geopolitical qualification criteria could lead to adverse reaction by other governments. ▪ A proliferation of separate QLs in any given area may pose difficulties for entities seeking qualification, especially if the evaluation criteria and qualification methods are disparate.

While there are many examples of Approved Products Lists and QLs throughout government and industry today, there are opportunities to reduce substantial risk to the ICT consumer by developing and implementing evaluation criteria that focuses on the supply chain risks associated with the manufacturer of the product and the entity that sells or provides the product or service.

This report can be used by organizations to identify circumstances under which the use of a QBL or a QML when purchasing ICT products or services may be appropriate. In addition, it explains how to mitigate ICT supply chain risks. It also provides supply chain risk management criteria and considerations to be used in the qualification process. Listed below is a use case example that describes SCRM resilience criteria that could be incorporated into a QBL/QML.

Use Case: The information technology components and parts produced by these manufacturers will be used in implanted medical devices. A failure or mal-performance has the potential to cause death.

Criteria	Evidence	Verification / Validation	Reference Standard / Guidance
Designed-in fail-safe functionality	Device	Device Testing by Independent Third-Party	Technical Documentation
Designed-in redundant functionality	Device	Device Testing by Independent Third-Party	Technical Documentation
Acceptable results of a stress test	Device	Device Testing by Independent Third-Party	Technical Documentation

RESOURCES

- ICT Supply Chain Risk Management Task Force: CISA.gov/ict-scrm task-force
- National Institute of Standards and Technology (NIST) Special Publication 800-161: https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final