MITIGATING ICT SUPPLY CHAIN RISKS WITH QUALIFIED BIDDER AND MANUFACTURER LISTS

Recommendations on the Use of Qualified Lists and Considerations for the Evaluation of Supply Chain Risks

April 2021

This page is intentionally left blank.

MITIGATING ICT SUPPLY CHAIN RISKS WITH QUALIFIED BIDDER AND MANUFACTURER LISTS

Recommendations on the Use of Qualified Lists and Considerations for the Evaluation of Supply Chain Risks

Executive Summary

As Information and Communications Technology (ICT) products and services evolve to provide increasing functionality, the supply chains that deliver them continue to grow more sophisticated and complex. Often hundreds of entities in multiple countries contribute in some fashion to a final product, from the mining of rare earth metals to the production of processing chemicals to sophisticated integrated circuits and software. The complexity and, to a degree, the proprietary nature and obscurity of ICT supply chains have made them increasingly at risk. This includes risk of exposure of sensitive or classified data that may imperil an organization's mission. There are currently no uniformly agreed upon and broadly adopted security standards, assurance standards, or criteria to evaluate the ICT products or processes to develop and produce them. The scope of this working group centered primarily on security and cybersecurity risks, not general risks (e.g., assurance of supply and labor compliance).

Cyber supply chain risks arise from threats to and through ICT. When an organization acquires an ICT product or relies upon an ICT service, they inherit these ICT cyber supply chain risks and their potential exposure to harm. With few exceptions, organizations rely upon ICT to perform their functions, and to process, store, and share data and information. As the criticality of these functions, or the value or sensitivity of their associated information increases, so does the level of trust an organization needs to have in the person or product performing a critical function, or that has access to important information.

Establishing and utilizing vetted, qualified sources of supplies can limit an organization's exposure to risk. Incorporating cyber-SCRM-focused qualification criteria into existing or new qualification list processes can provide a targeted and effective means for providing assurance that an ICT supplier or product is sufficiently trustworthy.

The Cybersecurity and Infrastructure Security Agency's (CISA) ICT Supply Chain Risk Management (SCRM) Task Force established the Qualified Bidders List (QBL)/Qualified Manufacturers List (QML) Working Group (WG3) with the goal of providing 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.

This report is the result of the efforts by the QBL/QML WG3. It 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.

Contents

Tables

Figures

QUALIFIED BIDDERS LIST (QBL)/QUALIFIED MANUFACTURERS LIST (QML) WORKING GROUP MEMBERS

LEADERSHIP TEAM FOR WG3:

	Name	Company
Co-Chair	Angela Smith	GSA
Co-Chair	David George	HP
Co-Chair	Emile Monette	Synopsys
Co-Chair	Jon Amis	Dell
Co-Chair	Savannah Schaefer	CompTIA

WG3 CONSISTS OF THE MEMBERS LISTED BELOW:

Name	Company
Chris Boyer, Jon Gannon, Rich Mosely	AT&T
Aaron Cooper, Meghan Pensyl, Thomas Ross	BSA
Charlotte Lewis	CDW-G
David Mazzocchi, Dwight Steiner, Kathryn Condello, Melissa Brocato-Bryant, Tammy Hamdy	CenturyLink
Eric Wenger, Joe Beel, Tammy Sanchez	CISCO
Bruce Raven	Dell
Jeffery Goldthorp, Steven Carpenter	Federal Communications Commission
Keith Nakasone, Kelly Artz, Larry Hale, Thomas Smith	General Services Administration
Trey Hodgkins	Hodgkins Consulting
Alvin Chan, Thomas Gardner	HP
Sam Ceccola	HPE
Jessica Sweet	Hunter Strategy
Courtney Lang, John Miller, Kelsey Kober	Information Technology Industry Council
Sampak Garg	Juniper
Amanda Craig, Christi Cox, Cindy DeCarlo	Microsoft
Kanitra Tyler	National Aeronautics and Space Administration

Jon Boyens	National Institute of Standards and Technology
Evan Broderick, Evelyn Remaley, Megan Doscher	National Telecommunications and Information Administration
Matt Tooley	NCTA
Jeremy McCrary	Office of Management and Budget
Coleman Mehta	Palo Alto Networks
Gary Banfield	Rehancement Group
Larry Ogintz	River Winds Computing
Kelley Misata	Sightline Security
Major Clark	Small Business Administration
Carol Woody	Software Engineering Institute - Carnegie Mellon University
Chris Jensen, Jamie Brown	Tenable
Robert Arnold	ThreatSketch
Colin Andrews	TIA
Drew Morin, Tanya Kumar	T-Mobile
Stacy Bostjanick	U.S. Department of Defense
Beatrix Boyens, Dennis Martin, Ronald Clift	U.S. Department of Homeland Security
Quynh Tran, Rebecca Adams, Scott Friedman	U.S. DHS, Cybersecurity and Infrastructure Security Agency
Scott Morrison	U.S. Department of Justice
Grace Motto, Michael Saperstein, Robert Mayer	US Telecom
John Conroy	Venable, LLC
Anita Patankar-Stoll, Frank Frontiera, Steve Baum	Verizon Wireless

BACKGROUND AND APPROACH

This report details the approach, findings and recommendations of the CISA ICT SCRM Task Force's Working Group 3 (WG3). WG3 was tasked to make recommendations on the potential use of Qualified Lists to help mitigate cyber risks associated with ICT supply chains.

WG3's overall goals were (1) to identify circumstances under which use of a QBL or a QML when purchasing ICT products or services may be appropriate to help mitigate ICT supply chain risks and, (2) to suggest supply chain risk management criteria and considerations to be used in the qualification process. The recommendations in this report are intended to be relevant and informative for both public and private sector purchasers and providers of ICT products and services.

For purposes of this report, WG3 uses the term "Qualified List" or "QL" to mean a list of suppliers or products that are approved for a given use based on meeting specific criteria. The scope of WG3's work focused on a qualified bidder or qualified manufacturer, qualification of a bidder or manufacturer, as those terms are defined in the Federal Acquisition Regulation (FAR).[1] However, QLs can and do also include Approved Products Lists (APL) as defined by policy, regulation, or guidance,[i] or any other list of suppliers or products that have been deemed compliant with certain criteria and approved for a particular use.

Qualification and listing in a QL is the process by which (1) products are obtained from manufacturers or distributors, examined, and tested for compliance with specification requirements, or (2) bidders, manufacturers, or other suppliers, are provided an opportunity to demonstrate their abilities to meet the standards specified for qualification. Following qualification, the names of successful products, manufacturers, or suppliers are included on lists evidencing their status. Generally, qualification is performed in advance and independently of any specific procurement action.

As part of a comprehensive Cyber Supply Chain Risk Management (hereinafter "C-SCRM")[ii] approach, organizations may require a higher level of confidence that a manufacturer or a supplier offering a service or a product are able to satisfy specific supply chain-related quality, security, integrity, or resilience objectives. An effective C-SCRM strategy should employ a multi-faceted, defense-in-depth/breadth approach designed to mitigate against a spectrum of potential supply chain risks. A QL that incorporates a holistic set of C-SCRM qualification criteria can be an effective way to provide positive assurance that a business entity, or the products and services a business entity offers or produces, is sufficiently qualified to be considered an acceptable source of supply for a particular use case.

WG3's recommendations are intended to:

- Serve as a reference source to raise awareness and educate both government and industry about (1) the purpose and benefits of QLs for ICT products and services, and (2) the importance of incorporating C-SCRM considerations into QLs;
- Provide actionable recommendations to incorporate C-SCRM into new and existing ICT-related QL criteria and program processes; and
- Promote the use of security or assurance standards as criteria to evaluate ICT products and services, and the processes used throughout their lifecycle.

[i] See, e.g., Dept. of Defense policy 8100.04 and the Unified Capabilities Requirements 2013 Change 2, available at https://aplits.disa.mil/processAPList.action, and the Federal Information Processing Standard 201 Evaluation Program, available at https://www.idmanagement.gov/sell/fips201/.

[ii] Cyber Supply Chain Risk Management is a systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing risk response strategies to the cyber supply chain risks presented by the supplier, supplied products and services, or the supply chain.

To accomplish this task, WG3 began by exploring the concepts and historical use of QLs, researched and examined the characteristics and requirements associated with QLs and qualification process activities, and developed a list of factors that can be used to inform an organization's decision to build or rely on a QL. A compilation of the background information on QLs may be found in Appendix A. Additionally, some illustrative examples of QLs may be found in Appendix D.

WG3 reviewed several current uses of QLs by the U.S. federal government. These use cases are representative examples and provide insights into the variation in criteria and processes that exists among and between existing federal QLs.[iii] As part of the analysis, WG3 examined the extent to which each QL program incorporates C-SCRM criteria. WG3 identified areas of overlap in requirements across the various QL programs and performed a gap analysis of each QL program's overall approach to C-SCRM. A summary of these use case reviews can be found in Appendix C.

The threat categories and the scenarios articulated by the CISA ICT SCRM Task Force's Threat Evaluation Working Group (WG2) provide valuable information to help organizations frame and inform their understanding of what can be done to guard against supply chain threats. WG3 determined the processes and controls used by an organization to mitigate against the myriad of these potential threats could be reviewed to determine whether those activities address risks appropriately. It was clear that while some processes or controls address specific threats, others are broad and often mitigate multiple threat categories.

After mapping the identified processes and controls to the WG2 threat vectors, WG3 then mapped the controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161[2] into the nine threat categories identified by WG2.[iv]

Due in large part to the difficulty posed by mapping threats and controls, a substantial effort was made to determine the best way to categorize the various risks that needed to be addressed by an acquirer of ICT products or services. After a thorough analysis of the output from WG2 on the various threats related to suppliers, it was determined that each of the threat categories mapped to the four pillars of supply chain risk outlined in NIST SP 800-161: security, integrity, resilience, and quality. In order to appropriately address supply chain risks, the protections in place for the bidder or manufacturer should appropriately and adequately address these pillars.

Each pillar was then analyzed to determine what criteria could be considered when developing a QL for the acquisition of ICT products and services. This process was informed by standards, guidelines, best practices, the use cases, and the subject matter expertise of task force members.

This approach offered valuable insight into when and how to use a QL in support of a procurement action and aided in optimizing the categorical groupings of C-SCRM criteria. It also revealed potential gaps and disparities related to control category coverage relevant to C-SCRM.

[iii] The use cases analyzed include the U.S. Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM), the National Aeronautics and Space Administration's (NASA) Solutions for Enterprise-wide Procurement (SEWP), the General Services Administration's (GSA) Second Generation Information Technology (2GIT) blanket purchasing agreement, the Department of Defense's (DoD) Enterprise Software Initiative (ESI) and the DoD Information Network (DODIN).

[iv] The WG2 categories are counterfeit parts, external attacks on operations and capabilities, internal security operations and controls, system development life cycle (SDLC) processes and tools, insider threats, economic risks, inherited risk (extended supplier chain), legal risks, and external end-to-end supply chain risks (natural disasters, geo-political issues).

CONSIDERATIONS FOR USE OF QUALIFIED LISTS TO ENHANCE C-SCRM

Qualified List Benefits

The primary benefits to using QLs are increased assurance that a supplier or product is sufficiently trustworthy, procurement efficiency, greater market certainty, and promotion of supply chain security practices.

Use of a QL can increase the efficiency of the procurement cycle by reducing the time needed for requirements definition, proposal evaluation, and source selection. All of which can reduce operating costs for buyers and suppliers by eliminating redundant activities for repeated purchases of the same type of ICT.

Use of a QL provides greater market certainty for ICT suppliers by making the buyer's specifications and evaluation criteria more transparent. This transparency promotes cost avoidance, increased return on investment, and improved fidelity of a supplier's cost-benefit analysis and other business decision-making. This can lead to increased competition and reduced prices for the buyer.

Use of a QL can also help promote and proliferate the use of desirable security practices, as suppliers seek to achieve the favorable position of being included on a QL. Modern commercial ICT products are designed once, manufactured to that specification, then sold many times using the same design and manufacturing processes. Any changes to the design and manufacturing process to adapt to unique requirements of a particular customer drives up cost. As a result, many commercial ICT manufacturers prefer to maintain a single design and production basis for ICT products, and they avoid developing unique design and manufacturing processes for individual buyers. However, if a supplier decides to universally incorporate certain C-SCRM controls and processes into its product design and manufacturing processes in pursuit of a "Qualified" designation, then all buyers of that ICT product are beneficiaries of increased security, not just the user of the QL. Similarly, ICT service providers that incorporate C-SCRM practices into their business operations ensure that all customers are the beneficiaries of increased security beyond the user of the QL.

In many cases, there may be third-party certifications that can be relied upon to demonstrate a party's ability to comply with certain requirements (e.g., the International Organization for Standardization (ISO) 27001 information security standard). This may allow a company to potentially gain or progress towards a position on a QL, while the evaluation of these specific criteria can be delegated to experienced, qualified professionals who grant such certifications.

Qualified List Costs and Risks

Creating a QL requires an investment of time and resources. If done properly, the return on this investment pays dividends. Over time the benefits can extend across teams, organizations, and even across government and industry. Additionally, building a QL program requires a provision of ongoing resources for management of the list. QL management may include processes for suppliers to be added or removed to the list, and to ensure that those on the list maintain conformance with the criteria of the QL.

A well designed QL can save time, money, and valuable resources. A poorly designed or maintained QL may jeopardize the success of the mission by potentially allowing the procurement of materials that can introduce risks, security threats, lack of availability or logistical capability, legal liability, or other factors.

The initial construction of a QL requires an understanding of the appropriateness and applicability of qualification criteria, as well as the capability and capacity to conduct an evaluation in a fair and

consistent manner, using a defined and accepted standard. The criteria must be selected and tailored to satisfy the purpose for which the qualified list exists, and the evidentiary requirements, verification, and validation, means and methods should be commensurate with the level of assurance needed. The evaluation of an ICT supplier seeking qualification likewise requires that there are evaluators with expertise in the domain area of the qualification criteria.

A QL is an ongoing programmatic endeavor rather than a point-in-time effort that can be closed, once completed. Any QL will require an ongoing assignment of resources to maintain and update it. The bulk of the effort may be in the initial creation of the list, but particularly in the ICT arena, there are dynamic factors that must be monitored that will require the QL process and requirements to be reviewed and refined after it is established. There may be legal requirements that require new entities be allowed to apply to join the list. Emerging technologies, risks, or other factors may cause the addition, deletion, or changing of requirements and a resulting re-evaluation of entities against the changes. The entities themselves may change as a result of mergers, acquisitions, or other factors which may precipitate a need for removal from the list. Ensuring that a QL is current and not reliant on obsolete data is critical to managing risk.

Overreliance on a QL can also engender a potential false sense of security. Purchasers may be tempted to assume that the QL accounts for a broader range of risks than it does, causing the purchaser to assume more risk than intended. While the best advantage of a QL is resource savings across organizations, such cross-organizational reliance of a QL must be made transparent to prospective QL users and entities seeking to become qualified. In addition, organizations that choose to rely on a QL must review the requirements and processes used for the QL before adoption to ensure that the qualification criteria will support the organization's security goals. Ideally, such organizations should be able to provide feedback on the QL program, where appropriate, so that the QL program becomes a superset of the best knowledge and experience of the organizations using the list.

Finally, any QL program can have geopolitical implications. Failure of an entity to earn a position on a preferred list could be met with reciprocal approaches or actions by other governments or organizations, particularly if insufficient transparency or procedural concerns create the appearance of protectionism or punitive action. A procurement team should be aware of potential implications when such a list is established, develop mitigations where feasible, and review such context periodically as part of the management program. In summary, the table below lists a range of benefits, costs, and risks associated with QLs:

TABLE 1: SUMMARY OF BENEFITS, COSTS, AND RISKS ASSOCIATED WITH QUALIFIED LISTS

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 CDM 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.

Establishing Qualified Lists: Considerations and Best Practices

When evaluating whether a QL can be an effective tool for managing supply chain risk, decision-makers will need to consider a range of factors relating to the need, intended use, viability, and cost of establishing and maintaining such a list. These factors should inform thinking about whether a QL is a feasible option for specific bidding or manufacturing entities and how to establish a QL to meet specific needs.

Considerations

Considerations about whether to establish a QL can be divided into those considerations relating to the *need* for such a list and those relating to the *feasibility* of establishing such a list in a manner that is practical and sustainable. Considerations informing how to establish a QL can be divided into those relating to *governance* of the list; those relating to *qualification* of covered articles or entities to be included on the list; and those relating to the handling of not-qualified or dis-qualified (*adverse) decisions* about applicants to the list.

- ***Need:*** Considerations include whether there are compelling risk-based reasons for seeking higher assurance for the potential list target; whether a given category of products, services, or systems will be purchased on a recurring basis; and whether existing policies and processes are adequate to manage supply chain risk in relation to the list target.
- ***Feasibility:*** Considerations include whether there are sufficient standards or other sources to guide objective evaluation of the list target; whether there is sufficient infrastructure for the maintenance of the list and the evaluation of the list target; and whether maintenance and implementation of the list is cost-effective.
- ***Governance:*** Considerations include:

    - How a list will be managed, maintained, implemented, and overseen; how to align a list with existing legal, regulatory, and international treaty obligations,
    - Which office(s) or program(s) will be responsible for those functions,
    - How information generated through processes associated with the list will be managed,
    - How will the list be made available or shared, by whom and to whom, and
    - Once in use by multiple organizations or projects (which is the main benefit of developing such a list), what is the process to either transfer governance and maintenance, or discontinue use, if the originating project team or organization is no longer able to maintain the list.
- ***Qualification:*** Considerations include how processes will be structured to enable evaluation and certification, and recertification; how qualification decisions will be communicated to applicants and to the public.
- ***Adverse Decisions:*** Considerations include how adverse decisions will be communicated to impacted parties; processes for arriving at, appealing, and rescinding or expiring adverse decisions.

Best Practices

Organizations establishing a QL should follow applicable best practices, unless exceptional circumstances dictate otherwise:

- Develop and use a risk-based approach and clearly define the scope of any certification and pre-approval schemes.
- Recognize certification and pre-approval schemes are not a replacement for overall cybersecurity and supply chain risk management.
- Leverage public and private multi-stakeholder communities' expertise and ensure transparency and information sharing.
- Reference global, industry-led standards and best practices as the technical basis for certification and pre-approval schemes to avoid technical trade barriers.
- Consider alternatives to third-party certification, including manufacturer self-declaration of conformity or vendor attestation and first-party assessments.
- Avoid localized testing and leverage mutual and multilateral recognition schemes.
- Adopt fair and transparent implementation.
- Strive to agree upon standardized criteria for risk measurement.
- Leverage related work in quantifying and qualifying risk:
    - Safety engineering and determining probability of outcomes
    - Risk assessments and probability
    - Shortcomings of methods for quantifiable assurance

Organizations should also be aware of emerging or new approaches to address C-SCRM risks, such as:

- SAE AS6171 counterfeit detection standard: Percent assurance based on threat coverage from laboratory testing and measurements
- Attacker/defender models utilizing Game Theory
- Distributed Ledger Technology (Blockchain technology applied to manufacturing data)

Purpose and Value of Addressing SCRM in a QL

As part of a comprehensive SCRM approach, organizations may seek a higher level of assurance that a product, its manufacturer, or a bidder offering a service or a product can be trusted. While trustworthiness is an attribute often assigned to a person, ICT SCRM practices and controls provide a

foundation upon which the characteristics of trustworthiness can also be applied to an ICT organization (e.g., bidder, manufacturer) or an ICT product or service.

As noted in NIST SP 800-161, "ICT SCRM lies at the intersection of security, integrity, resilience, and quality." As such, the attribute of trustworthiness can be understood to be a holistic representation of an inter-dependent combination of these four elements. In other words, being able to have adequate trust in a supplier, and the supply chain associated with their ICT service or product requires knowing, with sufficient certainty, whether:

- Quality standards are met;
- What you are acquiring is authentic and not tainted or otherwise compromised in some way;
- Information and assets associated with ICT are secure or securable;
- The items procured are sourced ethically and legally from upstream suppliers to the degree required; and
- The service or product will be resilient when under stressful conditions.

Manufacturer or supplier assurance measures the demonstrated ability of a manufacturer or supplier to satisfy identified supply chain-related security, integrity, resilience or quality objectives. Similarly, product assurance measures the degree of confidence that a product conforms to an acceptable standard that incorporates controls to address supply chain risk.

When incorporated into a qualification list activity, evidence that these assurance requirements are satisfied can provide a buyer or user of the ICT with a level of confidence that the supply chain controls are sufficient and that the resulting risk level is acceptable. The requirements should be informed by analysis of the criticality or sensitivity of an asset or function, supply chain threats, the likelihood of an attack, existing vulnerabilities that affect the likelihood of a successful attack, and the potential impact of a successful attack.

In addition to cybersecurity, there are ICT products whose assurance of uninterrupted or timely supply, timely availability, or replacement in case of failure is essential to the mission. A disruption or risk to the availability or quality of a product, or failure of a provider to deliver ICT products or services in accordance with agreement, can present risks to the mission beyond direct cyber threats. Including a measure of resilience to supply chain disruption is an important consideration in SCRM requirements.

Trust

Trust is a concept. It is not something easily measured, nor defined. Rather, it is built and gained – often over time – by a demonstration of the characteristics and behaviors that allow one to have confidence that something or someone can be relied upon and is aligned to or supportive of your needs and interests.

Supply Chain Risk Categories

As described in the approach section, WG3 examined how best to categorize the various risks that needed to be addressed by an acquirer of ICT products or services. The scope of this workstream effort focused on supply chain threat and cybersecurity aspects of these risks rather than other important, but separate, supply chain risk issues such as assurance of supply and timeliness of delivery. After a thorough analysis of the output from WG2 on the various threats related to suppliers, WG3 found that each of the nine threat categories mapped to the four pillars of supply chain risk outlined in NIST SP 800-161: security, integrity, resilience, and quality. Effectively addressing supply chain risks across the supply chain and life cycle of ICT requires that the protections in place for the bidder or manufacturer appropriately and adequately address the overlap of these pillars.

To provide focused attention to particular aspects of those pillars, the pillars were broken down into the following risk categories for the purposes of this effort:

- Supply Chain Security
  - Physical Security
  - Cyber Security
  - Personnel Security (inclusive of Company Leadership)
- Supply Chain Integrity
  - Hardware Integrity
  - Software Integrity
- Supply Chain Resilience
- Supply Chain Quality
  - Supply Chain Management and Supplier Governance

WG3 recognizes these risk categories can be categorized under more than one pillar. For example, the entire category of system development life cycle (SDLC) processes and tools could have been placed under Supply Chain Security or Supply Chain Integrity, but WG3 determined that for our purpose it fit best under Supply Chain Quality. While not called out explicitly as its own category, WG3 included considerations related to foreign ownership, control, and influence (FOCI) in the Personnel Security category, within the sub-category of geopolitical transparency. Protecting Controlled Unclassified Information (CUI) and classified information are included in the Cyber Security category within the sub-category of protecting customer information. Originally, the team categorized SDLC processes and tools under Supply Chain Quality (to focus specifically on the aspects of the process up to the completed design). Ensuring that the design was executed as expected, and that the product was not subject to tampering prior to delivery was the planned focus for the Supply Chain Integrity category. However, given the degree of overlap in controls between those two categories, WG3 decided to include the SDLC processes and tools within the Supply Chain Integrity category, with separate break outs for Hardware Integrity and Software Integrity. While reasonable arguments can be made for different categories or alignment of topics to categories, the grouping or location of these risk categories within a particular pillar is not particularly important. Rather, the objective is to ensure each of these topics are appropriately addressed within the larger context of ensuring supply chain risk is being effectively identified, assessed, and well-managed.

CATEGORICAL SCRM CONSIDERATIONS AND RECOMMENDATIONS

Supply Chain Security

This section addresses concerns for ensuring adequate physical security, cybersecurity and personnel security. Combined, these three areas of security focus provide a layer of defense that guards against exposure to a supply chain threat. A deficiency in any one domain can create a gap in protection that can undermine the effectiveness of the controls in place for the other domains.

PHYSICAL SECURITY

The physical security domain covers a wide range of activities that mirror the NIST Cybersecurity Framework (CSF) to include identify, detect, protect, respond, and recover. The traditional guards, gates, and guns description of physical security fails to capture the introduction of technology to monitor physical spaces, movements, and environmental conditions. For organizations that produce tangible goods, a traditional risk has primarily been theft. Today, the risk to ICT has expanded to include physical access to products or parts for the purpose of affecting their integrity. For example, gaining such access to ICT might be the target of adversaries seeking to implant malicious functionality. Integrated risk management, therefore, is the desired criteria.

The relative recency of cybersecurity as an independent branch of security (that may in some cases compete for resources dedicated to physical security) has created gaps that red team exercises have exploited. For the purposes of a QL, there should be considerations of how the organization seeking to be qualified, holistically addresses physical, cybersecurity, and personnel as well as addressing cooperation between these three domains.

Elements of Physical Security

Physical security addresses not only the protection of an organization's output, but the organization's assets, including intellectual property, staff, and even the local community surrounding a facility. A responsible organization takes such protection seriously and has mature processes backed by polices, rules, and procedures. Specifically, there are processes that address facility security, products in transit, and safety. Processes and activities all need to be considered in the context of risk components (i.e., vulnerability, threat, and consequence).

Physical security can be mapped to the five overarching functions of the NIST CSF: identify, detect, protect, respond, and recover. Such a mapping includes the following elements:

IDENTIFY	• Critical physical and information/data assets that need the greatest level of protection • Information/data that is of high value to adversaries or criminals or sensitive such as personnel or financial information • Weaknesses in existing physical security practices • Opportunities to engage with cybersecurity peers to promote teamwork • Peer (supplier, customer) organizations that have physical security risks
DETECT	• Probing for weaknesses, particularly when such probing is coordinated with a cybersecurity event • Breeches of a boundary or perimeter even when it appears that there is nothing disturbed
PROTECT	• Critical assets and people first; other priorities as determined by organizational leaders • Cybersecurity and signal paths of physical security protection systems (e.g., intrusion, access control, video monitoring systems) • Recognize distraction and diversionary tactics by adversaries and malicious insiders • Engage in design activities when a facility will be changed or a new facility is being considered to include how to deter, deflect, and detect adversarial activity
RESPOND	• Distinguish rules for an immediate response versus when to observe while coordinating with cybersecurity teams or another agency • Have a 24/7 response capability whenever a critical asset or sensitive information is under the protection of the physical security organization • Practice response coordination with both internal departments and external agencies
RECOVER	• Contribute to restoration of services and normal business processes whenever possible • Recognize the vulnerability of the organization when chaotic situations lead to ad hoc behaviors and actions that are contrary to the goals of physical security. Plan for them

Considerations for QBL/QML Criteria

Physical security criteria for QLs will rely primarily on adherence to existing laws, standards, industry best practices, and mature organizational physical security practices. Examples of these include, but are not limited to:

- Customs and Trade Partnership Against Terrorism (CTPAT): The CTPAT program details minimum security criteria for third-party logistics providers. These include "Customs and Trade Partnership Against Terrorism (CTPAT): "…documented procedures to screen prospective customers for validity, financial soundness, the ability of meeting contractual security requirements, and the ability to identify and correct security deficiencies as needed."[3]
- Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53): The standard for compliance with the Federal Information Security Management Act (FISMA) but also a reference for any organization to have mature, well-defined controls for all aspects of organizational security and privacy.
- National Industrial Security Program Operating Manual (NISPOM) and Department of Defense (DoD) Regulation 5220.22-M: Publicly available guide to how the government protects its most critical assets, information, and facilities where they reside.
- Transported Assets Protection Association (TAPA) standards: Facility Security Requirements (FSR) and Trucking Security Requirements (TSR)
- Other organizations that produce standards that include elements of physical security: ISO; ASIS International

CYBERSECURITY

Evaluating the security of a supplier's networks and related systems that enable an organization to run its day-to-day business, and connect them with their supply chain partners, is a foundational part of any determination of a qualification process. The evaluation of how a supplier protects its customer's data and its own proprietary data is also essential.

One means of guiding such evaluations is the application of the NIST CSF. Some of the sixteen Critical Infrastructure Sector Coordinating Councils[4] have developed and published CSF Profiles, designed to meet the unique needs of the particular sector.[5] For QLs focused on a given sector, these profiles will be especially appropriate, and may be able to be used with little or no tailoring. However, even for QLs that are not sector-specific, these profiles can also provide a useful starting point for determining which practices to include as criteria in the anticipated QL.

Other NIST publications that are useful when determining criteria to use in a QL to evaluate suppliers' cybersecurity posture are:

- NIST SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations: This publication provides guidance to federal agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels of their organizations. The publication integrates ICT SCRM into federal agency risk management activities by applying a multitiered, SCRM-specific approach, including guidance on assessing supply chain risk and applying mitigation activities.[6]
- NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations: This publication provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human

errors (both intentional and unintentional). The security and privacy controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk.[7]

- NIST 800-171 Protecting CUI in Non-Federal Systems and Organizations: This publication provides federal agencies with a set of recommended security requirements for protecting the confidentiality of CUI when such information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry.[8]

Measuring compliance with these standards may not represent a complete assessment of an organization's security posture, but it is a necessary step in the process. What is also a necessary step is determining what information requires protection, and at what level.

The foundational level established for the federal government, and for organizations that the federal government authorizes, to handle or store information that requires some level of information confidentiality protection is CUI. Below we examined that standard, how is it being administered, and how it impacts SCRM.

CUI and the Cybersecurity Maturity Model Certification

CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies, but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. Generally, this is information related to a program or contract that, if disclosed, could provide technical or proprietary information that would cause a security risk to the related program, contract or mission area. Executive Order 13556 called for the standardization of handling of unclassified information that still requires safeguarding or dissemination controls and established the National Archives and Records Administration (NARA) as the executive agency for efforts to manage CUI in the federal government. NARA has issued an Implementing Directive, 32 CFR Part 2002, and a Federal Acquisition Regulation to finalize these new requirements has been proposed, but not finalized.

The theft of intellectual property and sensitive information from all U.S. industrial sectors due to malicious cyber activity threatens economic security and national security. Malicious cyber actors have targeted and continue to target the Defense Industrial Base (DIB) sector and the supply chain of the Department of Defense (DoD). The aggregate loss of intellectual property and controlled unclassified information from the DoD supply chain can undercut U.S. technical advantages and innovation as well as significantly increase risk to national security.

As part of multiple lines of effort focused on the security and resiliency of the DIB sector, the DoD is working to enhance the protection of the following types of unclassified information within the supply chain:

- Federal Contract Information (FCI): FCI is information provided by or generated for the Government under contract not intended for public release.
- Controlled Unclassified Information (CUI): CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended.

DoD promulgated Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting" which requires contractors to provide adequate security on all covered contractor information systems, to include, as applicable, compliance with the security requirements in NIST Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

After implementation of DFARS 252.204-7012, DoD issued an interim rule on September 30, 2020, to amend the DFARS to implement the DoD NIST SP 800-171 Assessment Methodology and the Cybersecurity Maturity Model Certification (CMMC) framework to assess contractor implementation of cybersecurity requirements and enhance the protection of controlled unclassified information within the DoD supply chain. The interim rule went into effect on November 30, 2020. The Department is in the process of reviewing public comments to the interim rule to inform the final rule which is expected to be published later in 2021.

The CMMC framework adds a certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. The CMMC program is designed to provide increased assurance to the DoD that a DIB contractor can adequately protect FCI and CUI at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain.

The CMMC model sets forth five levels of cybersecurity maturity and aligns a set of processes and practices with the type and sensitivity of unclassified information to be protected and the associated range of threats to include advanced persistent threats (APTs). CMMC Level 1 is focused on the protection of FCI and encompasses the basic safeguarding requirements set forth in FAR clause, 52.204-21. CMMC Level 3 is focused on the protection of CUI and encompasses the security requirements from NIST SP 800-171 as well as certain additional cybersecurity practices and maturity processes. CMMC Levels 4 and 5 further include a subset of the enhanced security requirements from the NIST SP 800-172 "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171" as well as additional cybersecurity practices and maturity processes.

To facilitate a smooth transition to CMMC, DoD is implementing a phased rollout over a five-year period. The CMMC requirements will apply only to a subset of new contracts, task orders, or delivery orders awarded from November 30, 2020 through September 30, 2025. On or after October 1, 2025, all DoD contracts will include CMMC requirements. The following are additional details:

- From November 30, 2020 through September 30, 2025, if inclusion of CMMC requirements in the solicitation is approved by the Office of the Under Secretary of Defense for Acquisition and Sustainment, a DoD vendor must be certified at the CMMC level required by the solicitation to be eligible for award at either the prime or subcontractor level, excluding solicitations solely for the acquisition of COTS items or micro-purchases.
- On or after October 1, 2025, all DoD vendors must be certified at the CMMC level required by the solicitation to be eligible for award at either the prime or subcontractor level, excluding solicitations solely for the acquisition of COTS items or micro-purchases, which level is intended to be, at minimum, CMMC Level 1.

The program manager or requiring activity will determine the CMMC level for a specific contract, and the prime contractor will flow appropriate CMMC requirements at the level that is appropriate for the information that is being flowed down to the subcontractor.

Application to Supply Chain Risk Management

CUI is relevant to SCRM because the information that is critical almost always includes information or technical data. This data may be encountered or developed as items or components move

through the supply chain toward inclusion as part of a good that could be a commercial item or part of a system in a weapons platform or other major defense acquisition program. Efforts to protect the confidentiality of information and technical data of items as they move through the supply chain are covered by the CUI initiatives. Contractors providing those items to DoD are required to establish and maintain certification of compliance with the underlying standards.

PERSONNEL SECURITY

Personnel security addresses the need to ensure people and companies (which are owned, controlled, and influenced by people) do not pose an unacceptable security risk.

As companies' human resources departments determine personnel levels and types of positions to hire or outsource to contractors, it is important to understand the scope of the individual positions, the criticality of that position in the company to carrying out its duties, and to review the risk associated with positions in collaboration with cybersecurity professionals, IT, and potentially, legal counsel. Determining and documenting risk levels for each position is a good step and includes defining the scope of a role, whether the role should be broken into multiple roles, and the access to and impact someone could have on an organization's (whether their own or someone else's) data or systems. This includes physical or logical access to personnel data, financial files, intellectual property, or other sensitive information. Proper vetting of personnel and due diligence on their background checks is critical to address risks related to what that person will do (i.e., their role) at the company and their scope of influence in the position.

Organizations also need to enforce segregation of duties and have effective oversight mechanisms in place to detect anomalous behaviors or actions by personnel. Such anomalies might include, for example, exceeding their access, abusing their connectivity, connecting unauthorized equipment to the network, or attempting to visit sensitive areas that are not part of their normal workspace.

Companies are competitive by nature. Not only are companies competing on products and services, they are competing for talent. Often, in small to midsize companies, talented personnel can take a lot of valuable corporate knowledge with them when they leave. Requiring non-disclosure or non-compete agreements is one way to mitigate against the risk of this knowledge being used or shared in a way that is detrimental to the person's former employer.

Nation-state actors often attempt to fulfill positions within companies to gain access to sensitive corporate secrets, access to facilities, and access to government contracts and government facilities. Often, these positions are in sensitive technology related positions that can be hard to fill. They can also be non-technical positions, such as custodial staff, that tend to have access to many rooms of a facility when they are less populated and draw little attention. Specialists or highly skilled personnel, at lower price points are found and solicited to contractors that provide key personnel to such programs. Companies should be aware of and sensitive to identifying methods such as this that may be used by a Nation-state actor to plant an employee within an organization. If and when such red flags arise, this should prompt the organization to proceed cautiously and apply additional scrutiny before hiring someone.

Understanding these types of risks, the scope of duties, and when people will have access to certain information (direct or indirect) will help in scoping whether a position is at the right risk level and can help improve the development of personnel policies and scope of duties to minimize and address such risks.

Authorized personnel can also have nefarious intent and capabilities, making them an insider threat. This often represents the greatest risk to a company. In addition to reviewing and assigning risk to each position, organizations need to be aware of the behaviors and characteristics typical of an insider threat actor. If possible, having an insider threat program will also help address aspects of this concern.

A well-thought-out approach to personnel security, including fostering a culture of threat awareness, is an important component of personnel security. It requires multiple components of HR, legal, contracts and acquisitions, physical security, cybersecurity and IT to work together to develop and implement personnel security policies, practices, and monitoring capabilities that help in protecting an organization from supply chain threats.

Security risks may also arise from the ownership or managerial layer of a company and its personnel. These are people that may have a leadership role, own or have a controlling interest in a company, or are otherwise able to wield influence over the company. It's important to examine the factors that will point to whether the company is a responsible source of supply (such as financial health, compliance with laws or safety practices, etc.), and whether there is any potential security risk that may arise due to the people that own, control, or may influence the company.

SCRM Considerations for QBL/QML Criteria

Qualification criteria should address whether and how a supplier ensures personnel security needs are satisfied.[v] Companies need to demonstrate effective policies and procedures to properly vet potential employees, including background and reference checks, as appropriate. In addition, they should conduct periodic vetting of existing employees and to discern whether anything has changed that could now place the employee in a riskier position. These qualification requirements should also flow down to sub-tier suppliers.

Information about a supplier's management team, its ownership and managerial structure, and the personnel that own, control, or may influence the supplier should also be obtained during the qualification process.

Additional criteria might include:

- A requirement for a formal insider threat program.
- Evidence that all employees receive regular training in how to handle sensitive information as well as training about cybersecurity attack vectors, such as phishing, so they may be alert to it and not victimized by general attacks, and so that they may more easily recognize and report potential breaches of security.
- Employees with direct and regular access to sensitive information receive training relating to handling such information and proper maintenance, and destruction when appropriate, of sensitive data.
- In some instances, a requirement for qualification as a bidder might include providing evidence that work will only be performed by U.S. citizens.
- A bidder may also need to demonstrate that there are adequate personnel security controls in place for their sub-contractors or other relevant third-party entities.

SUPPLY CHAIN INTEGRITY

Hardware Integrity

This portion of the report is specifically dedicated to hardware assurance, and more specifically relates to hardware integrity. While there may be some concern about *hardware confidentiality* (who can see your design or build of materials) or *hardware availability* (is the product and source of the product reliable enough to maintain its predictable supply through the supply chain), there is specific concern about how to measure and manage *hardware integrity*. An acquirer or user needs to have a

[v] For additional control and reference information pertinent to personnel security, please see the current versions of NIST SP 800-53, NIST SP 800-161, and resources available at: https://www.dcsa.mil/ (e.g., information about background investigations, insider threat).

sufficient level of confidence that the hardware being designed or acquired can be trusted to function as intended.

This is part of the *quantifiable assurance* and *zero trust* challenge we face today. Organizations need to be able to answer the question: what evidence must be collected and presented over the lifecycle so that the user can trust the hardware, to some degree, to perform as expected (even in cyber contested environments)?

There will always be missions, functions, and programs which require higher assurance or trust levels than others. One can look at the confidentiality, integrity, and availability with three levels of risk: high, medium, and low. The risk manager prioritizes and integrates these for his/her risk model. This weighting, prioritization, and integration by organizations' leadership is part of the *governance* process described in this report. How the developer, supplier, and user can and will measure or rate (and collectively agree to measure) all the components of a system is a difficult challenge. As described below, there are a variety of techniques in use, and being developed, to establish minimum *compliance* and abilities to further rate hardware integrity in a risk-based-approach to managing overall approach to cybersecurity.

Elements of Hardware Integrity in ICT SCRM

Hardware integrity is not a well-defined area—especially for a full computer, circuit-board, keyboard, mouse, sensor, actuator, or any other product or system composed of and enabled by information technology sub-components—but that definition should be a goal for developers of those products and parts.

The relatively new Common Weakness Enumerations for Hardware (HW-CWEs)[vi] construct is described as, **"…**a community-developed list of common software and hardware weakness types that have security ramifications." "Weaknesses" are flaws, faults, bugs, vulnerabilities, or other errors in software or hardware implementation, code, design, or architecture that, if left unaddressed, could result in systems, networks, or hardware being vulnerable to attack. The CWE List and associated classification taxonomy serve as a language that can be used to identify and describe these weaknesses in terms of CWEs.

Targeted at both the development and security practitioner communities, the main goal of CWE is to stop vulnerabilities at the source by educating software and hardware architects, designers, and programmers and acquiring on how to eliminate the most common mistakes before software and hardware are delivered. Ultimately, use of CWE in development of QL criteria can help prevent the kinds of security vulnerabilities that have plagued the hardware and software industries and put enterprises at risk.

CWE helps developers and security practitioners to:

- Describe and discuss hardware and software weaknesses in a common language.
- Check for weaknesses in existing hardware and software products.
- Evaluate coverage of tools targeting these weaknesses.
- Leverage a common baseline standard for weakness identification, mitigation, and prevention efforts.
- Prevent software and hardware vulnerabilities prior to deployment.

[vi] https://cwe.mitre.org/about/index.html. The CWE is broken down into the following categories: Manufacturing and Life Cycle Management Concerns; Security Flow Issues; Integration Issues; Privilege Separation and Access Control Issues - ; General Circuit and Logic Design Concerns - ; Core and Compute Issues -; Memory and Storage Issues - ; Peripherals, On-chip Fabric, and Interface/IO Problems -;Security Primitives and Cryptography Issues - ;Power, Clock, and Reset Concerns - ; Debug and Test Problems -; Cross-Cutting Problems

Risk management personnel should also consider measures to mitigate risks associated with firmware, and the integrated circuit or microchip. Tamper resistance, watermarking, and obfuscation are some examples of leading-edge security practices the risk manager may want to consider.

While hardware assurance/hardware integrity (HWA/HWI) does not have a holistic schema to verify assurance or integrity, there are standards and controls that can be leveraged to develop a QL. A description of some of these sources can be found in Appendix E.

Counterfeit Protection

Having a QBL/QML helps prevent counterfeit by using authorized suppliers, wherever possible, and integrating them into the organization's supply chain. There are a number of techniques that exist to protect against counterfeiting and copying integrated circuits (IC).[vii] The simplest is to employ a fully trusted foundry for production that is able to guarantee the use of procedures that combat tampering. However, such foundries are expensive and may lack the advanced processes needed to produce competitive commercial devices.

One option to reduce cost is to use split manufacturing, in which different foundries are used to produce different layers of the IC. That way, a single foundry cannot tamper with the design and be assured that it will work with the other foundry's production. But split manufacturing may still be cost-prohibitive for general use ICT such as office computer and print equipment. Split manufacturing is also at odds with the most efficient interfaces used for fabless production and entails finding foundries with front-end and back-end processes that are compatible with each other.

The move to three-dimensional integrated circuitry (3DIC) production may provide one answer.[viii] Another method, that involves less supply-chain overhead, is to alter the circuit design to make it less amenable to overbuilding, counterfeiting or copying. Logic encryption, for example, inserts logic gates at key points in the design that are wired to a register. Unless this register is loaded with the correct key, the IC will not function correctly. Layout analysis could also be used on a de-capped chip to determine register values that will work, so encryption may need to be used in combination with camouflaging or circuit obfuscation, which is normally employed to prevent reverse engineering of the circuit intellectual property.

SCRM Considerations for QBL/QML Criteria

As recommended by the CISA ICT SCRM Task Force, the acquirer should buy from Original Equipment Manufacturers (OEMs) whenever possible. This helps the acquirer or user better answer questions of pedigree and provenance, and is today, the single best general mitigation for a variety of general hardware integrity threats.

Developers and managers of QLs seeking to address hardware security should consider including a requirement for suppliers to provide a bill of materials (BOM) that includes data about pedigree and provenance of the item being purchased.

[vii] While it is beyond the scope of this paper to address all the various risks and mitigations that can be taken, some other measures include, for example: establishing a strong visual inspection regime on all received ICs or acquiring a certified first production run item directly from the original IC manufacturer.

[viii] For example, at the 22nd Usenix Security Symposium in August 2013, Frank Imeson and colleagues from the University of Waterloo received the best student paper award (https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_imeson.pdf) for their proposal to use technology to prevent an attacker based at a foundry from successfully inserting a Trojan. Their idea was to obfuscate the integrated circuit by 'lifting' selected circuitry to a trusted tier which would be fabricated at a trusted location while the remainder of the chips in the stack would use the conventional foundry supply chain. The method developed by Imeson and colleagues allows the 'trusted' layer to be no more complex than a passive interposer.

To mitigate counterfeit hardware, consider a QL requirement that suppliers use a trusted foundry, split manufacturing, 3DIC, or logic locking in development and production of the microelectronics that will be included in the final product.

To address known weaknesses and vulnerabilities in hardware, consider a QL criterion that suppliers address all CWEs applicable to the hardware being purchased (or some portion of, e.g., all critical and high impact).

Software Integrity

Unlike the hardware or product supply chain, the software supply chain exists in a digital realm that appears much more abstract, but presents no less, and possibly even more, security threat vectors to ICT than the hardware supply chain.

In developing a QBL or QML which include components to address SCRM, qualification requirements that address the software supply chain should be considered. While there are fewer applicable standards and common practices to reference, there are software security measures that can be employed and demonstrated as being in place. There is a distinction between ensuring the software product itself is secured and ensuring the security of the supply chain system to deliver the software product (note that we are addressing only the latter).

Software security is a broad discipline that covers secure development and lifecycle maintenance of software as well as security capabilities and features included in software. Software supply chain security represents just one dimension of software security, and generally includes the management of third-party components and systems used to develop and deploy the software, including the development environment and tools used therein. While the security of the software itself and its susceptibility to malicious manipulation in regular use are most certainly of critical importance, that is not the scope of these recommendations or this task force. Here we limit the discussion to the process of creation and delivery of the intended product, not the integrity of the intended product itself.

Elements of Software Supply Chain Risk

Though the concept of a software supply chain is fluid, at least four elements should be considered in evaluating software supply chain risk: (1) security of the development environment in which software is created; (2) management of third-party components integrated into a code base; (3) security of the systems and processes used to reproduce and deploy software or transmit software code to users; and (4) security of the systems and processes used to transmit and receive software updates and patches to software which is already deployed.

The software development environment includes the network environment, systems, tools, and databases used to produce, compile, test, and store software code. It includes the tool chain—tools such as compilers or development frameworks—as well as code repositories.

Modern software relies heavily on the integration of third-party components including both proprietary and open-source components. Larger software projects may often be composed of as much as 80% third-party components. These components often include subcomponents or dependencies that can be incorporated by software developers with limited knowledge of their existence, provenance, or pedigree. Ineffective management of third-party components represents a significant potential risk, as third-party components may include known vulnerabilities or may be targeted by malicious actors to introduce vulnerabilities, which then can be incorporated into the software project.

Software can be deployed in several different ways, including on hard disc, an internet download, or in the form of cloud-based Software-as-a-Service (SaaS). Software deployment can be a source of

risk when security measures are insufficient to prevent product tampering or counterfeiting, or unauthorized access to deployment environments (often cloud-based containers or similar virtual environments).

Finally, software developers may depend on cloud and server infrastructure to deploy updates or patches to software and incorporate technical measures to enable software to verify or receive such updates or patches. Risk can be introduced if either transmitting or receiving mechanisms are insufficient to prevent unauthorized access, tampering, or introduction of malicious code including the possible counterfeiting of updates or patches.

Managing the Four Elements of Software Supply Chain Risk

Some or even many of the components of an effective hardware ICT SCRM program may, and should, also be applied to software and mitigate all four categories of risk. These include items such as physical security and personnel security of the development environment where software is created, vetting of companies for secure development practices and other potential risk, management of subcontractors and sub-suppliers, a secure development lifecycle, application of anti-tampering protections, and methods for verifying authenticity of the product. A software supply chain, however, will also have some different requirements. Key controls for addressing the four areas of software supply chain risk are as follows:

Software Development Environment:

- Risk-based cybersecurity frameworks, such as the NIST CSF, should be applied to development environments.
- Identity management and access controls should be applied to allow only authorized changes, and prevent unauthorized access, to software code.
- Tool chains should be configured to secure settings and should be updated to the most recent versions.
- Change management tools should log relevant information (e.g., time and date, authorized user, reason) for each change to the software code. Use of digital signatures to validate the authenticity of each revision is encouraged.

Third-Party Component Management:

- Software developers should maintain an up-to-date inventory of third-party components, including—to the extent practicable—an inventory of subcomponents and dependencies indirectly incorporated via third-party components, as might be listed in a Software Bill of Materials (SBOM), for example.
- Third-party components should be subjected to standard code review and testing procedures to identify known vulnerabilities and ensure seamless integration with the broader code base.
- Software developers should, where possible, vet suppliers, establish trusted repositories of third-party components, and enforce security standards through contracts.

Software Deployment:

- Software should be deployed with supplier source certification or authentication indicators and should protect those indicators against tampering and counterfeiting.
- Software should include measures, such as code-signing or anti-tamper measures, to protect the software's integrity and prevent counterfeiting.
- Supply chain data should be protected at rest and in transit against unauthorized access.

- Containers and other virtualization technologies used to deploy software should be securely configured.

Software Updates:

- Update servers should be securely configured, and common cybersecurity protections should be applied to prevent unauthorized access to servers.
- Software updates should be cryptographically signed.
- Software should be capable of validating the authenticity of a patch or update.
- No update should contain push authorization which could direct a system to a third-party site for authentication, rather all updates should be signed and accompanied by an independent pull to a trusted site to verify and authorize the update.

Inventory of Software and the Utility of a Software Bill of Materials (SBOM)

In order to address the four elements of supply chain risk for software across a complex ICT system, it is important for an acquirer to understand the software components delivered as part of a system or product.

These components may include all the applications with direct interfaces to the user; the operating system in which the applications execute; additional system management tools and utilities or middleware that may be included in the system; subsystems components such as device drivers for monitors, sensors, or accessories which may not be part of the operating systems; and below this level, the system firmware, Basic Input/Output System (BIOS), and other lower level code. Many applications, and some management tools, may not reside locally on devices itself but rather be maintained remotely in the cloud and may remotely access, or be accessed by, local devices, or may operate across devices ("peer to peer") in an ICT system. Each component of software represents a potential point of attack, and a complex system such as a server or a laptop may contain hundreds of software components.

For this reason, a QL requirement may include a requirement for an inventory of software components incorporated into an ICT system. It may also include the provisioning by the bidder or manufacturer of an SBOM. An SBOM lists the software components of an ICT system and their source. The level of detail required may vary by mission or use case. Some software developers are beginning to publish an SBOM, providing a list of components and subcomponents to customers, but no consensus standard for an SBOM exists yet. Also, it may not be possible to list the source of every line of code in every software component of a complex ICT system, and some details may not be available due to IP or legal restrictions. This is a promising area and the National Telecommunications and Information Administration's (NTIA) multi-stakeholder process is assembling guidance to advance its maturity.

SCRM Considerations for QBL/QML Criteria

QLs should be constructed to ensure that a qualified software manufacturer should meet the above criteria, and a qualified bidder should only use manufacturers and suppliers that meet these criteria. Further, just as semiconductor devices should only be purchased from OEMs or their authorized resellers, rather than open market brokers, software should only be purchased from OEMs and their authorized resellers.

Evaluation of these criteria should be informed by existing standards and best practice guides. In particular, the NIST White Paper on a *Secure Software Development Framework* (SSDF)[9] and BSA The Software Alliance's *BSA Framework for Secure Software*[10] each offer technical guidance on software security that includes software SCRM, with references to specific standards and

documentation where available. SAFECode's *Managing Security Risks Inherent in the Use of Third-Party Components*[11] provides detailed guidance on third-party component management.

Additional Considerations for Firmware

Firmware usually refers to fixed or semi-permanently embedded data integrated into a hardware device, whereas software is generally designed for user interaction. Firmware may include programmable logic embedded deep in the hardware [field-programmable gate array (FPGA) programming or read-only memory (ROM)], subsystem firmware and drivers, microcontrollers that may be preprocessing and analyzing sensor data (e.g., in a PC microphone provisioned with speech or keyword recognition), communication firmware as used in an ethernet or Wi-Fi module, system firmware and BIOS, and other technologies. Because of its position within hardware to control low level functions (e.g., voltage level on a power rail) and also its programmability, ability to potentially be updated remotely, and its roles in functions such as authentication, firmware lies in a position where it may be considered hardware or software depending on context. Many of the above risk mitigation strategies— including securing development environments, managing third-party components, and securely deploying updates—apply to firmware; however, additional considerations also apply. For example, a hardware secure root of trust should be present to establish a secure perimeter around, and secure execution environment for, BIOS and firmware components to prevent unauthorized or unsigned updates. Major firmware components should be included in an SBOM for an ICT system.

Supply Chain Resilience

Resilience can be defined as the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions. Threats or hazards that could result in harm to, or disruption of, an ICT supply chain or an ICT product or service (or service provider) itself are viable concerns that organizations which provide or use these ICT products or services must consider as part of a comprehensive approach to managing supply chain risk. While not all ICT products and services are critical, in many instances they are relied upon by organizations to perform a critical function. It may be imperative that certain ICT be able to withstand disruptions to ensure sustained operations or be able to resume operational capability quickly when disruptions or failures occur.

Taking proactive steps to better ensure resilience begins by understanding what products and services are most critical and then, systematically examining and assessing what is required to sustain or recover operational functions, if and when a disruptive or destructive event occurs. Risks that can impact the broader supply chain should also be considered to determine how best to build in redundancy and assurance that critical supply chain nodes, trade paths, and partners can be relied upon and will be sufficiently available, capable, and accessible.

The threats or hazards may vary but it can be reasonably assumed that there will be a need to assure resilience which can be measured by achievement of an acceptable minimal level of accessibility, availability, performance or functionality, and security. For ICT that is integrated into or connected to operational technology, safety is a key consideration.

In order to understand the risk each supplier faces, ensure consistent communication and dialog with the supplier, make sure adequate time is invested in supplier analysis, and build an adaptive and resilient supply chain. Below are sample questions that organizations can review to begin to better understand how best to address their resilience needs and potential vulnerabilities.

- Do cybersecurity controls align to the criticality of the function that the product or service provides? Are the controls the same for failover or back-up locations?
- Does the nature or purpose of a business or mission function or the ICT itself make it an attractive target of an adversary?

- If equipment needs repair or replacement, can it be obtained from reputable, trusted sources? Can it be obtained in a timely manner?
- Would any existing cybersecurity controls need to be adjusted to accommodate emergency operations or situational needs?
- How are new personnel (who may need temporary access during a continuity event to perform or support an ICT service) vetted? How are credentials issued and controlled?
- Is backed-up data sufficiently protected? Are storage locations physically safeguarded?
- How is the resiliency of ICT products considered (i.e., can the product function under stress)? Does the ICT have any fail-safe characteristics?
- Can contractors or supply chain entities be relied upon during an emergency or contingency situation?
    - Do contracts cover contingency operations?
    - What situations may affect contract scope or ability of contractor to perform as required?
    - Will increased costs be incurred?
    - Will the acquiring organization be able to provide needed direction/oversight?
    - Can additional or alternate contractor support be obtained if needed?
- Could interconnected ICT pose a cyber-supply chain risk? How would critical functions be impacted if inputs or outputs were compromised or not available?
- Are there any unique communication or coordination needs that should be considered? How would these be affected during a contingency situation?
- Will patching or upgrades occur in a timely manner?
    - Who is responsible for providing patches and for installing them?
    - Will there be any impacts to being able to scan for vulnerabilities or monitor and detect threats and incidents?
- What infrastructure disruptions would impair ICT (e.g., power surge, damage to equipment, loss of water, inability for employees or contractors to perform jobs, network services compromised, connected ICT possibly compromised)?
- Do alternate locations have same physical security protections or access controls as a primary site?

SCRM Considerations for QBL/QML Criteria

When there is a need to ensure certain SCRM resilience requirements are met with regard to certain types or categories of a manufactured ICT product or component or for a bidder of an ICT product or service, it may be appropriate to consider incorporating these requirements into the criteria and qualification process of a QBL/QML.

The following are some example use cases that describe SCRM resilience criteria that could be incorporated into a QBL/QML (Note: Criteria, Evidence, Verification/Validation Method; and Reference Standard/Guidance should be understood to be illustrative examples only):

Use Case #1: The government relies upon an outsourced service for the sustained performance of a mission critical function. To ensure continuity of operations, any disruption or failure of this function must be fully recoverable within 12 hours or less.

CRITERIA	EVIDENCE	VERIFICATION / VALIDATION	REFERENCE STANDARD / GUIDANCE
Bidder must have a continuity a plan that ensures capability to recover within the required timeframe	Continuity Plan	Third-Party Review or QL Program Activity Review; Continuity Tabletop Exercise or Real-Life Continuity Event Results	Federal Continuity Directive 1 and 2 (or equivalent)

Use Case #2: Bidder provides a Cloud Service Solution that is relied upon for multiple agencies of the government and must be continuously available 24/7.

CRITERIA	EVIDENCE	VERIFICATION / VALIDATION	REFERENCE STANDARD / GUIDANCE
Capability to sustain minimal staffing levels of vetted, qualified personnel at primary and back-up data centers	Staffing Plan; Key Personnel Resumes; Vetting Requirements and Processes	Third-Party/Qualified Program Activity Review	As determined by the Qualification Program Activity
Alternate Power Generation	Pictures; Documentation	On-site Verification; Bidder Certification; Third-Party/Qualified Program Activity Review	Alternate Power Generation Equipment shall be of sufficient capability and Fuel Source must be on-site or demonstrated to be readily attainable
Redundant Telecommunications	Documentation	Third-Party/Qualified Program Activity Review	Redundant Telecommunications Services, of sufficient capacity, must be in place and sustained and acquired from an alternate provider, unless this is not a verifiably available option
Back-Up Data Centers are geographically	Pictures; Documentation; Risk	On-site Verification; Bidder Certification;	Data Centers shall be diversely located to

dispersed, rely upon a separate part of the Energy Grid	Assessment Used to Inform Location of Facilities	Third-Party/Qualified Program Activity Review	mitigate against all potential natural risks (e.g., seismic, flood, fire, hurricane, etc.)

Use Case #3: 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

Use Case #4: Critical ICT replacement parts must be sourced from OEM and available on short notice. Geopolitical or natural hazard disruptions may impair operations at a specific facility location or its logistics processes or shipping paths. Alternate manufacturing sites and trade routes are necessary to mitigate against the risk of not being able to obtain required, critical OEM parts in a timely manner.

CRITERIA	EVIDENCE	VERIFICATION / VALIDATION	REFERENCE STANDARD / GUIDANCE
Manufacturer must have redundant and disperse manufacturing locations and alternate trade path options	Documentation	On-site verification; Third-Party or Qualifying Program Activity Review of Evidence	Facility locations must be in the more than one country/continent

SUPPLY CHAIN QUALITY

Supply Chain Governance and Control

Introduction

In addition to specific controls to manage known security risks in an ICT supply chain, many supply chain risks and threats, including those which may not yet be known, can be mitigated to an acceptable degree by generally strong ICT supply chain governance and management. Good governance implies adherence to consistent processes and improvement in those processes over time. It suggests strong organizational knowledge and management of upstream suppliers, business continuity, and measures to assure product quality. It demands efficient communication up and down the supply chain, whether for the purpose of managing information such as demand forecasts, managing cash through correct invoicing and accounting, or managing material and knowing what inventory is positioned where, within a complex global network. These capabilities and the relationships required to maintain them imply, if not explicitly assert, that threats or activities which may manifest as unexpected perturbations of the equilibrium of a smooth-running system are more preventable, more detectable, and if manifested, can be met with a more expedient and effective coordinated response, than if such overall governance is neglected or is not in place.

A QBL or QML that is designed to minimize ICT supply chain risk should assess the foundational supply chain governance on which more effective specific measures may be built as described elsewhere in this document, or as may evolve over time.

Many of these measures of governance listed below may be indirectly assessed through the presentation of a relevant certification, ISO-9000 being one example at the time of this publication, in lieu of additional rigor or presentation of documentary evidence of such practices.

SCRM Considerations for QBL/QML Criteria

Overall processes for accountability, upstream SCRM, and vendor onboarding and management:

- Presence of a documented quality management system (ISO 9001);
    - Tracking of customer quality and reliability metrics such as DOA (defects on arrival) and mean time between failures (MTBF)
    - Supplier quality management system such as incoming material inspection and measures to prevent use of counterfeit components or unauthorized substitute materials
- A system to flow down requirements and practices to sub-tier suppliers and hold them accountable;
- Documented sustainability policy and practices, including social and environmental responsibility (at minimum compliance with applicable laws and measures to prevent upstream suppliers from engaging in corruption, child labor, or other illegal activity);
- Existence of a documented SCRM plan or supply chain business continuity plans;
- Equitable division of responsibility and reasonable indemnifications;
- Meaningful warranty terms and conditions;
- Documented supply chain cybersecurity plan;
- (QML only): Does manufacturer conduct reviews of audits, summaries of test results, or other equivalent evaluations of critical suppliers/providers; and
- (QML only): Does manufacturer conduct response and recovery planning and testing with critical suppliers/providers?

Secure hardware and software (product) design and development practices as applicable (Note: For a QML, all of these are applicable; for a QBL, only applicable if bidder is designing a system or is also developing their own hardware/ software):

- Hardware design which may be integrated into a system security engineering approach outlined in NIST SP 800-160;
- Software development based on a Secure Software Development Lifecycle such as SAFECode, the NIST Secure Software Development Framework or ISO 27034;
- Effective Hardware and Software testing and validation practices;
- Building Security in Maturity Model (BSIMM); and
- Appropriate method to translate customer specifications to development metrics (speed, uptime, etc.) if applicable.

Service delivery processes and practices (if applicable):

- Digital transformation (new services, transition);
- IT cloud dependence or independence, or if transitioning from on-premise to cloud or vice-versa, plans for ensuring security of data and continuity of operations through transition;
- Help desk support;
- Data center management; and
- Service level agreements.

SUMMARY

As part of a comprehensive SCRM approach, organizations may seek a higher level of assurance that a product, its manufacturer, or a bidder offering a service or a product can be trusted. While trustworthiness is an attribute often assigned to a person, ICT SCRM practices and controls provide a foundation upon which the characteristics of trustworthiness can also be applied to an ICT organization (e.g., bidder, manufacturer) or an ICT product or service.

Building SCRM considerations into an ICT-focused QL can be an effective and beneficial means to assess whether a bidder or manufacturer is meeting applicable SCRM requirements.

WG3 recommends that qualification criteria related to one or more of the SCRM pillars, as described in this report, should be incorporated into ICT QLs.

APPENDICES

Appendix A: Background on Qualified Lists

WHAT IS A QUALIFIED LIST AND ITS PURPOSE?

QLs[ix] are intended to provide positive assurance that a business entity, or the products and services a business entity offers, is sufficiently qualified to be considered an acceptable source of supply, especially when there is a need for a higher level of assurance that qualification criteria have been met. Compared to what is available from the general marketplace, or even available from vendors who are authorized to contract with the federal government, a vetting process to qualify for inclusion on a list provides greater confidence that qualified businesses, and the services and products associated with a qualified business entity, have demonstrated conformance to a set of clearly defined requirements or standards. These requirements are tailored to address specific compliance, performance, or risk mitigation objectives specifically relevant to the purpose and scope associated with the need and justification that provided the basis for the establishment of the QL activity.

The Federal Acquisition Regulation (FAR) describes qualification and listing in a QL as "…the process by which products are obtained from manufacturers or distributors, examined and tested for compliance with specification requirements, or manufacturers or potential offerors, are provided an opportunity to demonstrate their abilities to meet the standards specified for qualification. The names of successful products, manufacturers, or potential offerors are included on lists evidencing their status. Generally, qualification is performed in advance and independently of any specific acquisition action.

WHO IS RESPONSIBLE FOR A QUALIFIED LIST?

Establishing and managing a list program, as well as the process to qualify and maintain qualification, typically involves numerous different organizations. While QLs are often associated with the acquisition process, an acquisition official's role is to justify the use of and leveraging of these lists. They do not define the qualification criteria, nor are they responsible for conducting assessments to determine qualification.

For example, DoD Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, requires that "*In applicable systems, integrated circuit-related products and services shall be procured from a trusted supplier accredited by the Defense Microelectronics Activity when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as application-specific integrated circuits)."*

The graphic below shows the various roles and relationships of the persons and entities typically associated with a QL program.

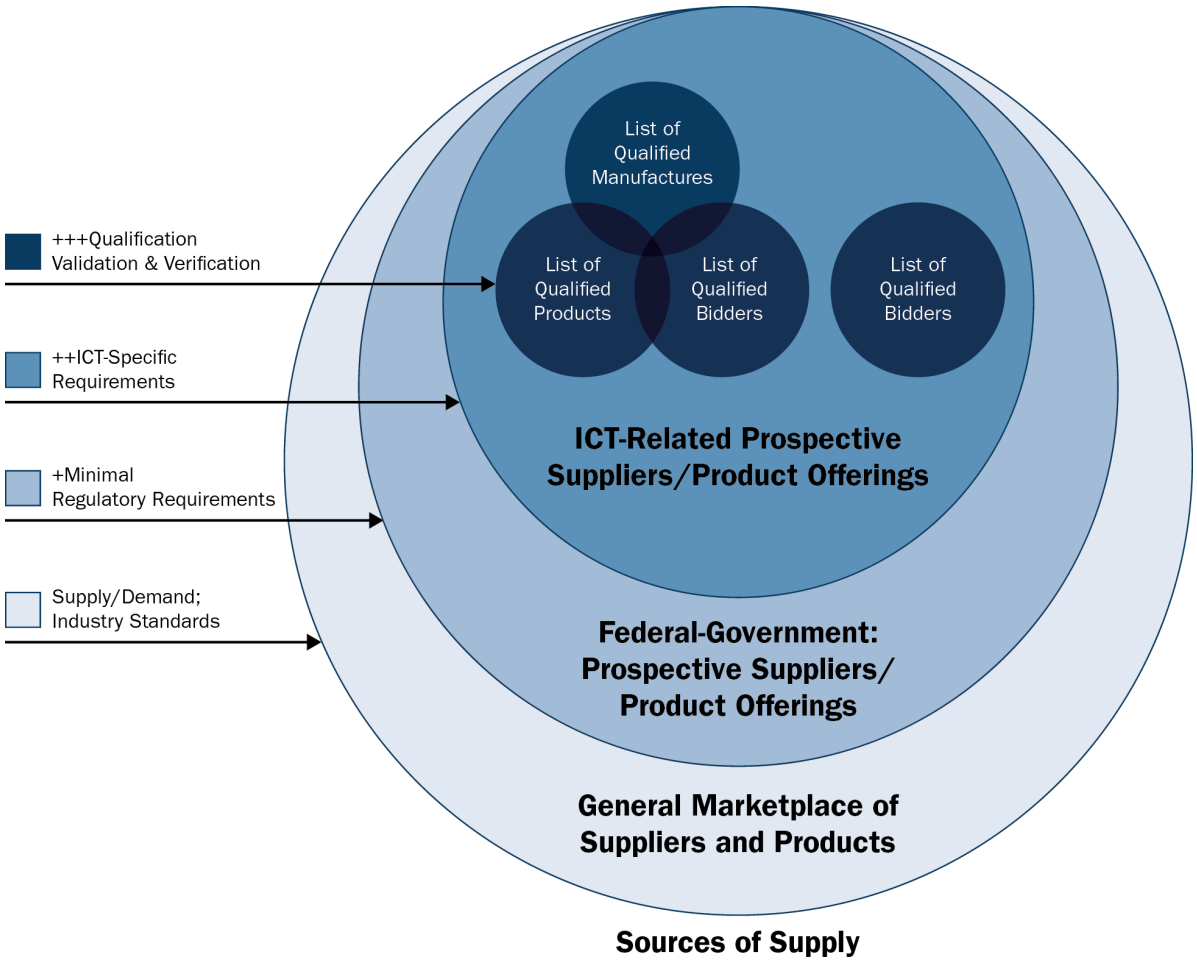
[ix] For purposes of this report, WG3 uses the term "Qualified Lists" to encompass [FAR Part 9 def]. In contrast to a qualified list, ineligible or prohibited entity lists include names of "ineligible" manufacturers, suppliers, or products and are intended to serve as a reference for identifying sources of supply that should not be used. Ineligibility can occur for varying reasons. For example, a company that has an "inactive" registration record in SAM.gov is not eligible to do business with the Federal Government but this does not mean they are banned or barred by the Government; rather, the company may have decided to shift its focus to the commercial marketplace or simply missed recertifying its registration record in a timely manner. In contrast, ineligibility can also occur because of national security concerns or violation of law. For example, an entity on the Specially Designated National (SDN) List, published by the U.S. Department of the Treasury's Office of Foreign Assets Control includes a list of individuals and companies owned or controlled by, or acting for or on behalf of, sanctioned entities. Their assets are blocked, and U.S. persons are generally prohibited from dealing with them.

FIGURE 1: ROLES AND RELATIONSHIPS ASSOCIATED WITH QUALIFIED LISTS

FIGURE 2: EXAMPLES OF RELATIONSHIPS BETWEEN QUALIFIED LISTS, PROGRAMS, AND ACQUISITION ACTIONS

- CISA' CDM Program -> List of Approved CDM Products List -> GSA Offers Approved CDM Products via Special Item Number (SIN) on GSA Multiple Award Schedule; Agencies purchase CDM tool from SIN via eBuy or GSAAdvantage
- GSA's FedRAMP Program -> List of FedRAMP authorized cloud services and products -> Agencies issue solicitation to sources that offer FedRAMP authorized cloud services or products
- DoE's Federal Energy Management Program -> QL of Energy Service Companies (ESCOs) -> the ESCOs are the solicitation sources (e.g., qualified bidders) solicited for energy savings performance contracting (ESPC) procurements
- DLA's Microcircuit Qualification Program -> Custom Hybrid Microcircuits QML -> Procurement of microcircuits must be from an approved source
- GSA IT Category Office -> IT Services/Products Blanket Purchase Agreement Awardees (qualified bidders) -> Agencies issue task orders to BPA awardees

FIGURE 3: VENN DIAGRAM OF QUALIFICATION LISTS, REQUIREMENTS, AND STANDARDS FOR SOURCES OF SUPPLY



FEDERAL ACQUISITION POLICY REGARDING QUALIFIED LIST REQUIREMENTS

The Federal Acquisition Regulation (FAR) spells out a set of prerequisite policy conditions that must be met before a new QBL, QML, or Approved Products List (APL) requirement can be established.[12] At a summary level, these include:

- The head of the agency that wishes to establish a QL must complete a justification for why a qualification requirement must be met prior to setting a requirement for a contract award.
- The justification must include an estimation of likely testing and evaluation costs that will be incurred by the entity seeking qualification.
- The complete specification of the set of least restrictive requirements that a potential offeror (or its product) must satisfy in order to become qualified.
- Qualified personnel who have no existing or potential conflict of interest and, as applicable, qualified facilities to perform an assessment as to whether qualification requirements are met and sufficiently objective specific to incorporated controls that protect against supply chain threats and reduce supply chain risk.
- Vendors must be told why their products or services did not satisfy the requirements for the QL.

- While a waiver exists under FAR Part 9.202, it does not apply to a QL.
- A contracting officer is not required to delay a proposed award for a vendor who is not on a QL.

WHAT VARIATIONS IN QUALIFIED LISTS EXIST?

WG3 focused its efforts on QBLs and QMLs, as defined by FAR and used by federal officials:

- QBL: 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 qualification requirements. (FAR Part 9.201)
- QML: List of manufacturers who have had their products examined and tested and who have satisfied all applicable qualification requirements for that product. (FAR Part 9.201)

Generally, a manufacturer refers to the creator of hardware or software products, platforms, or systems. In the case of ICT, this may include cyber-physical systems which contain IT or communication resources as well as ICT that performs a physical function (e.g., a printer, 3D printer, assembly robot, CNC machine, etc.).

A bidder refers to the direct provider of such a system who will deliver, install, and usually service and support a hardware or software system, and may also be responsible for integration of the system with existing equipment, cloud services, or new systems from multiple manufacturers.

Within the Federal Acquisition System, a bidder is the business entity seeking to enter into a contract with a federal acquirer to provide a good or service that entity is supplying. It is possible for an entity to be both a bidder and a manufacturer.

In addition to the federal government, QLs are also used by private sector organizations, state and local governments, as well as international organizations. There are numerous qualified-list variations, to include Qualified or Approved Product Lists, Lists of Accredited Suppliers, Qualified Supplier List for Distributors, Authorized Reseller Lists, and others.

Please refer to Appendix D for a representative sampling of these lists and QL program activities and organizations.

A QBL or QML may also be used to establish a list of providers for emerging or advanced ICT capability that is required earlier than a thorough product level qualification can be completed, or when a product level qualification is impractical prior to awarding a contract (e.g., a custom-built system). The bidder or manufacturer may be screened and monitored on a periodic basis for processes that reduce risk, specific SCRM (and other risk) mitigations, as well as historical data on presence of controls and capability to prevent threats and risks to the customer. In such a case, use of a QBL/QML can increase a buyer's confidence that risk has been mitigated, even in the absence of a product level qualification, though it must be noted that this is only one mitigation and does not guarantee complete immunity from supply chain risk, or any other risk.

BEST PRACTICES FOR QUALIFIED LIST BUILDING

Based on Widely Recognized Standards: To the greatest extent feasible, qualification should be based on evaluation of covered articles or entities against existing, internationally recognized standards. Such standards ease the bureaucratic burden on suppliers, ensure consistent results, and align evaluations against widely recognized best practices. Where such standards correspond to, and can be satisfied by, an industry certification, confidence is increased that the evaluation against the criteria was performed by an expert in the field on behalf of the certifying body. Below are illustrative examples of commonly used standards for ICT articles and entities.

USEFUL STANDARDS FOR EVALUATING LIST TARGETS	
List Target	**Standards**
Organization	NIST Framework for Improving Critical Infrastructure Cybersecurity; NIST SP 800-53; Open Trusted Technology Provider Standard (OTTP-S); ISO/IEC 27001, 27002, and 27034
Hardware or Firmware Product	NIST SP 800-161; IEC 62443
Software Product or Service	NIST White Paper: "Secure Software Development Framework"
Cloud Platform	FedRAMP; ISO/IEC 27000; SOC II Type 2

Broadest Possible User Base: QLs should be established to encompass the broadest possible user base. For common products, there may be broad benefit if lists are government-wide in scope. For mission-specific products, lists should cover all government agencies with similar mission requirements. Such lists should use a common data model to ensure consistency in the management of data. Such an approach ensures efficiency, can enable the government to obtain favorable pricing, and prevents contradictory or redundant requirements.

Transparent Decision-Making: Absent exceptional circumstances, QLs should be accompanied by processes that provide for the timely notification of impacted parties when a covered article or entity is the subject of an adverse decision, and list managers should ensure those processes are consistently implemented. Transparency creates public confidence in the integrity and sound management of the QL program and prevents confusion.

Robust Appeals Process: Absent exceptional circumstances, QLs should be accompanied by transparent processes that provide opportunities for impacted parties to appeal an adverse decision on a covered article or entity. The appeals process should enable impacted parties to present facts relevant to their appeal and obtain a timely decision from a qualified authority. Robust appeals processes create public confidence in the integrity and sound management of the QL program and prevent confusion. Furthermore, a robust appeals process may aid in the discussions necessary for appealing entities to become qualified even if not initially, expanding the pool of qualified suppliers to the benefit of the procuring organizations and teams.

Recertification at Reasonable Intervals: Recertification of articles and entities should be established based on the characteristics—including the rate an article is updated, an article's anticipated lifespan, and other factors—of the specific articles and entities covered by a QL. In all cases, recertification should be required only as often as necessary to maintain confidence that relevant risk is addressed. As a guidepost, the ISO/IEC 27001 requires recertification once every three years.

QUALIFIED LISTS SUPPORT GOVERNANCE, COMPLIANCE AND RISK MANAGEMENT OBJECTIVES

Incorporation of SCRM considerations into QL criteria and processes can provide an effective means to ensure both C-SCRM and compliance requirements are met. Organizations need assurance that the products and services they acquire, and use to align to business and mission objectives, fulfill their intended purpose, are trustworthy, and conform to standards and legal and regulatory requirements. A QL that includes SCRM considerations brings together aspects of governance, compliance, and risk management to create an increased level of assurance. Governance, compliance, and risk management are inter-related and complementary. All three help in attaining

desired outcomes by preventing or mitigating against undesirable results or behaviors and helping ensure acceptable baseline standards are met.

RELATIONSHIP BETWEEN GOVERNANCE, COMPLIANCE, AND RISK MANAGEMENT

Governance provides the leadership direction, structure, and processes that influence organizational culture and values and facilitates awareness, analysis of, and decisions about organizational priorities, resources, plans and actions, roles and responsibilities, and accountability. Compliance and risk information are necessary inputs to the governance function as they help to frame, and shape decision-making for governance outputs. These outputs, in turn, impact compliance and risk management priorities and practices.

Compliance is about satisfying a mandate. An assessment of compliance produces an answer that is either black or white about whether there is evidence of conformance to a standard, law or some other specific, objectively measurable, static requirement. Achieving compliance is typically within the bounds of an organization's control.

Risk management is a discipline that employs tools and techniques that can influence or help predict outcomes but cannot guarantee an outcome. In contrast to compliance, an assessment of risk will always lie in the grey area between the black and white and its measurement is based on ever-changing variables. The factors that affect risk are both internal and external to an organization and will never be within the full control of an organization. Risk is dynamic in nature. While its measure is informed by objective evidence, it is also influenced by context, timing, external factors, as well as the knowledge, experience, and the perspective of the assessor.

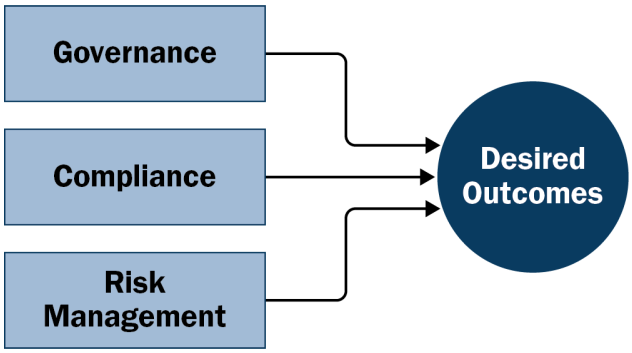


Figure 4: GCR Relationship

FIGURE 5: SIMPLIFIED DECISION MODEL FOR EVALUATION OF POTENTIAL QBL/QML

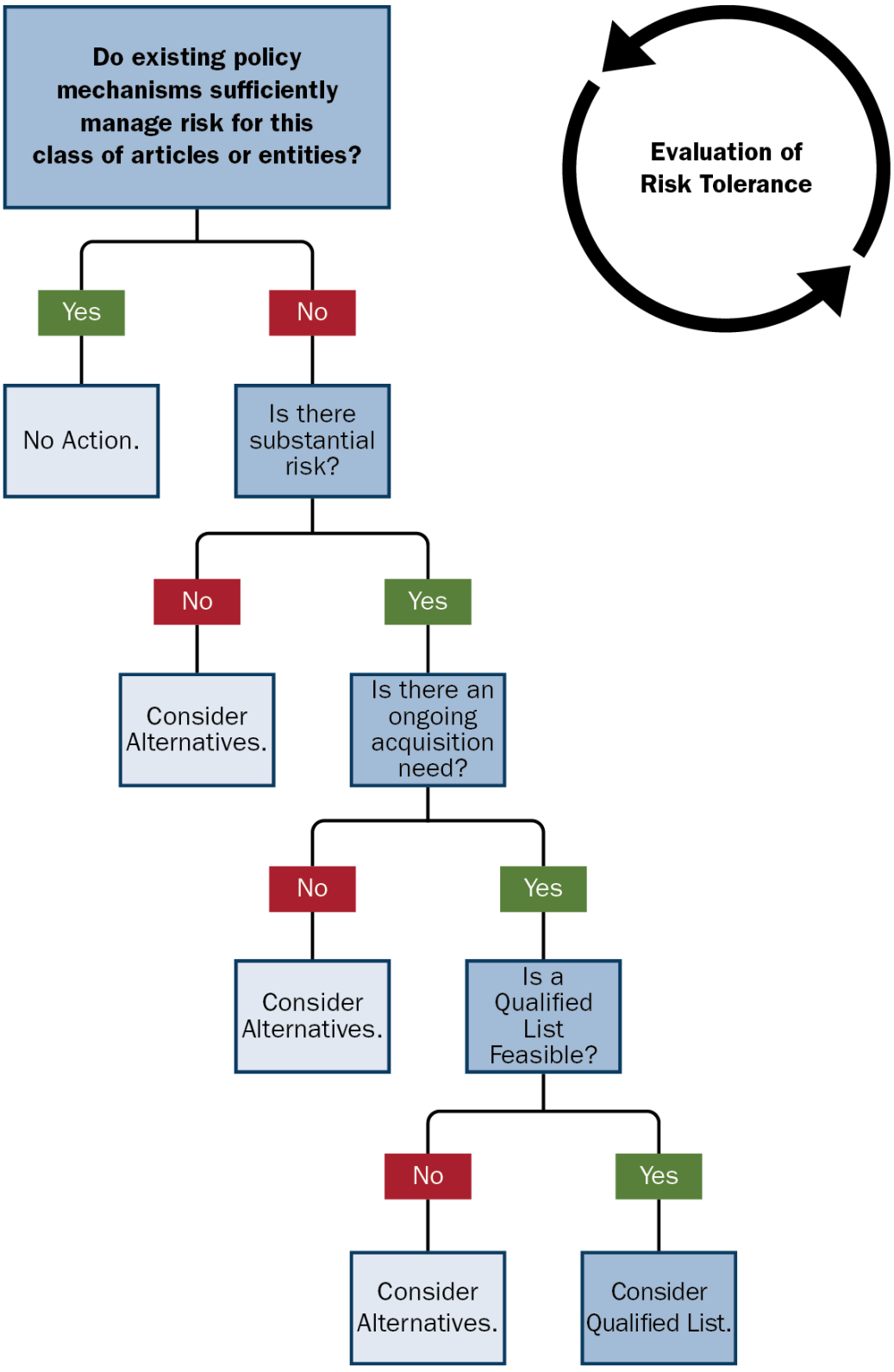


TABLE 2: WORKSHEET: EVALUATING THE UTILITY AND FEASIBILITY OF QUALIFIED LISTS

QUESTION	EXAMPLE INDICATORS	YES/NO
Is there a need for elevated assurance?	• Is the product, service, or system to be covered by the QL a national security system? • Is the product, service, or system to be covered by the list included on existing critical asset lists or supporting critical functions such as the High Value Asset (HVA) list or Agency Mission Essential Functions? • Is there specific information or intelligence indicating a threat or risk to the product, service, or system? • Are existing policies and processes governing the acquisition of the product, service, or system inadequate to manage supply chain risk?	
Is there an acquisition requirement?	• Will participating government agencies be making purchases of or from the list target on a recurring basis? • Will the list cover products, services, and/or systems with many available sources (vice custom-built items or items with limited sources)?	
Is a QL feasible?	• Does the responsible office or agency maintain sufficient capacity to maintain and implement the proposed list? • Can the list be established or maintained with available budgets and without exorbitant cost?	

TABLE 3: WORKSHEET: ESTABLISHING THE PARAMETERS OF A QUALIFIED LIST

CONSIDERATION	RESPONSE
Governance	
What is the purpose of the QL?	
What are the legal authorities, regulations, and requirements relevant to the list?	
Who is the intended user-base? Is it government-wide? Agency- or program-specific? Purpose-specific?	
What authority will oversee management and implementation of the list?	
What are the anticipated resource requirements for establishing and maintaining the list?	
How will information generated by processes associated with the list (e.g., sensitive intellectual property provided by manufacturers during qualification) be protected (e.g., from Freedom of Information Act requests)?	
To whom (e.g., what other government organizations) will information generated by processes associated with the list be made available?	
Qualification	
What is the scope of a qualification under the list? To whom or what, specifically, does the qualification apply?	
What standard(s) or source(s) will be used to evaluate the targets (products, services, systems, manufacturers, or bidders) of the list?	
What is the process used to evaluate the list targets for qualification (e.g., self-attestation, third-party certification)?	
Can qualification occur at different levels (e.g., Gold, Silver, Bronze)?	
Is qualification of a list target on a one-time basis, open-ended, or on some other basis?	
How often will the list targets be required to be recertified?	
Adverse Decisions	
What is the process for notifying an impacted entity of a decision to reject or revoke qualification?	
What will cause a qualification to be revoked (e.g., contract fraud)?	
What is the effect of revocation of qualification? • Does any disqualified product, service, or system installed on government networks need to be removed? • Who is responsible for the actions and cost triggered by disqualification?	

• How do disqualification decisions impact multiple products affected by the same issue?
What is the process for appealing a decision to deny qualification? What authority is ultimately responsible for evaluating appeals?
What is the process for appealing a decision to revoke qualification? What authority is ultimately responsible for evaluating appeals?

Appendix B: Additional Recommendations for Incorporating SCRM into ICT QLs

KEY PRACTICES

Federal agencies incorporating C-SCRM into QL programs should first identify the key practices that comprise an effective SCRM program, to ensure a consistent and comprehensive evaluation baseline. For instance, draft NIST IR 8276, *Key Practices in Cyber Supply Chain Risk Management,*[13] identifies eight key practices that make up a robust SCRM program:

1. Integrate C-SCRM across the organization
2. Establish a formal program
3. Know and manage your critical suppliers
4. Understand your supply chain
5. Closely collaborate with your key suppliers
6. Include key suppliers in your resilience and improvement activities
7. Assess and monitor throughout supplier relationship
8. Plan for the full lifecycle

Together, these key practices highlight the importance of vendors' ability to demonstrate end-to-end SCRM across the enterprise and across a product's entire lifecycle—design, sourcing, manufacturing, etc.—including the importance of demonstrated proactive actions to manage those risks and ensure product integrity. Supplier management in this context is critical, including close collaboration with suppliers to collectively manage risks and understanding geopolitical implications of manufacturing locations. A formalized SCRM program, bringing together personnel from supply chain operations, product management, and other corporate functions, and managed with an executive sponsor is a strong indicator of effective risk management.

These overarching key practices should be present in all organizations seeking QL qualification. However, when incorporating SCRM into a QL, agencies should recognize that vendors will adopt differing levels of each activity based on a risk-based continuum. Accordingly, individual QLs should set their own baseline levels for each key practice based on risk.

VALIDATION

When a QL is utilized for an acquisition activity, the Acquisition Team should also consider how to validate vendors' adherence to key SCRM practices, and how or by whom such validation should be carried out. In most sensitive ICT procurements, validation will go beyond self-attestation to include a mechanism for audit or review. For instance, the General Service Administration's (GSA) 2GIT program incorporates vendor proposed SCRM plans into each vendor's contract. Annual vendor risk assessments and program reviews, along with internal GSA quality assurance audits, are used to verify adherence to the SCRM plans. The Continuous Diagnostics and Mitigation (CDM) Program Management Office (PMO) implements a conformance and technical validation for applications to its Approved Products List (APL); successful conformance includes provision of a vendor's SCRM plan and completion of SCRM plan questionnaires. The CDM PMO leverages a federally funded research and development center to conduct an open-source review of products submitted for the APL for technical alignment and research into the product capabilities.

A crucial consideration is for agencies to ensure its validation mechanism evaluates the totality of a vendor's SCRM program, without resorting to a static checklist exercise.

LIFECYCLE CONSIDERATIONS

Agencies should determine the appropriate review lifecycle for qualified entities or products. These reviews may be done on an annual basis or can be triggered by a change in the risk posture of the

qualified entity or product or conducted more or less frequently based upon reporting and risk assessment outcomes.

When developing a QL, agencies should consider how often to conduct periodic reviews, and develop processes for addressing changes in status of qualified vendors. Agencies should also define what changes to a vendor's SCRM practices would result in a qualified status change and develop notification and appeal procedures for vendors to maintain or re-qualify for qualified status.

ADVERSE QUALIFICATION DECISIONS

Similarly, agencies should develop clear, transparent processes for issuing, communicating, and reviewing adverse qualification decisions. Among other considerations, agencies should determine what kinds of communications will occur with the applicant going through the evaluation process and identify clear procedures for adjudicating applications. Agencies should also develop clear processes for applicants to obtain information about, and appeal or challenge, adverse decisions. Agencies should have guidelines for applicants that are denied qualification and wish to re-apply.

In the case of GSA's 2GIT, vendors can only be reassessed for potential qualification when option years are exercised, and only if re-assessment is considered in the best interest of the government. On the other hand, the CDM PMO accepts, considers, approves, or rejects vendor submissions to its Approved Product List on a monthly basis, which enables the program to maintain currency and meet rapidly evolving cybersecurity requirements. Prospective vendors receive feedback from the PMO throughout the review process and may resubmit applications at any time.

Appendix C: Summary of Use Case Reviews

Throughout its first year, WG3 gathered information on a sample of five programs within the federal government, with input from working group members on comparable commercial practices. These programs provide for varying methods of addressing supply chain assurance. Basic descriptions of each are transcribed below.

CONTINUOUS DIAGNOSTICS MITIGATION (CDM)

The CDM program helps strengthen the cybersecurity of government networks and systems by providing federal agencies with cybersecurity capabilities and tools. DHS and GSA collaborated to create a CDM Tools Special Item Number (SIN) for GSA's Schedule 70 IT program, which includes commercial off-the-shelf (COTS) IT products that meet one or more of the CDM program technical requirements and are listed on the CDM APL. One of the APL qualification criteria is the completion of the required SCRM Plan (CDM Tools SIN, 2019). The full complement of CDM subcategories includes tools, associated maintenance, and other related activities such as training. The SIN is organized into five subcategories based on their CDM capabilities. The CDM Tools SIN features high-quality cybersecurity vendors offering products and related services to federal, state, and local governments.

Benefits:

- From the vendor perspective, the CDM Tools SIN (132-44) provide vendors an opportunity to apply to sell software and hardware solutions on a specialized cybersecurity program that is marketed to organizations throughout the federal government (CDM Tools SIN, 2019).

Benefits to vendors awarded the CDM Tools SIN include:

- Prioritization – CDM-sponsored requirements prioritize the use of CDM vehicles (CDM Tools SIN and CDM Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) are the preferred method for procurement, giving CDM Tools SIN holders an advantage of obtaining first consideration and opportunity to compete);
- Ease of Buying - The CDM product offerings are consolidated and categorized into product families for ease of discovery and access;
- Expedited Awards - The CDM program is eligible to use the GSA FAST Lane program to award and modify contracts quickly. New awards can take up to 45 days and modifications only a couple of days; and
- Ease of Adding Emerging Technologies – CDM allows for added flexibility and speed to market for emerging technologies.

Vendors that want to sell on the CDM Tools SIN must first get their products on the DHS APL. Once their tools are on the APL, vendors can then apply to be on GSA's CDM Tools SIN.

From the ordering perspective, federal government entities are ensured that the hardware and software products and associated services under this SIN undergo a CISA product qualification process in order to be added to the CDM APL. Ordering entities also have access to a vendor's submitted SCRM plans and can use this information to inform their procurement decisions.

Potential Opportunities for Improvement:

- Develop a process to continuously monitor and identify security concerns and to subsequently notify vendors, if or when their products have security concerns;
- Create a mechanism for communicating with ordering officials and vendors if or when a vendor's products have been placed on a Removed Products List (RPL) or if they are not recommended for government procurement;

- Define and communicate regarding the frequency for conducting periodic re-evaluations;
- Mature the process for vendors to mitigate identified security concerns and then re-apply for consideration on the CDM APL; and
- Periodically review and refine SCRM plan requirements.

GENERAL SERVICES ADMINISTRATION (GSA) CATEGORY MANAGEMENT

GSA IT Schedule 70 is a government-wide, multiple award, contract vehicle that delivers federal, state, and local customer agencies the tools and expertise needed to shorten procurement cycles, ensure compliance, and obtain the best value for innovative technology products, services, and solutions. The vehicle facilitates the purchasing of more than 7.5 million products and services from over 4,600 vendors. GSA awards and administers Schedule contracts containing basic pricing, terms and conditions as well as oversee authorized ordering activities under Schedule contracts for specific requirements.

The IT Schedule 70 not only provides quick access to pre-vetted, experienced providers, but it also simplifies the procurement process and allows for the ordering Agency to have complete control over their task orders. Schedule 70 contracts include standard clauses and terms and conditions to ensure supplier compliance with the FAR. Importantly, this schedule enables a flexible awarding system for socio-economic groups, set-asides, and task order level Service Level Agreements (SLAs).

Benefits:

- Vendors have the opportunity to offer a wide variety of products and services from which federal entities can then order,
- Competitive prices and discounts,
- Maximum order threshold,
- Flexible contracting and streamlined ordering,
- Includes security solutions, and
- Approved Agreements with End-User Licensing Agreements (EULA)/Commercial Supplier Agreement (CSA).

Potential Opportunities for Improvement:

Include baseline, minimal SCRM requirements for ICT products and services. Specifically, ensure the vetting process for vendors includes a baseline assessment of supply chain risk. Ordering agencies could then build upon this baseline assessment and tailor their task order requirements, based upon the criticality and risk level associated with their particular procurement.

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) 201 EVALUATION PROGRAM AND APL

The Office of Management and Budget (OMB) issued Memorandum M-06-18 that requires federal agencies to procure only qualified products and services listed on the GSA APL when implementing HSPD-12 into their environment. Procurement of approved products and services facilitates the government-wide objective of a federated and interoperable Federal Identity, Credentials, and Access Management (FICAM) segment architecture, and ensures compliance, consistency and alignment of commercially available products and services with the requirements and functional needs of FICAM implementer.

The APL provides federal agencies with products and services that have been approved for FICAM implementation based on rigorous security vulnerability and interoperability testing performed by the FIPS 201 Evaluation Program (ID Management, 2019). Product testing evaluates and certifies services and commercial products used in credentialing systems, physical access control systems, and public key infrastructures. Product testing is performed by either third-party accredited testing

labs or GSA-managed testing labs. OMB Memorandum M-05-24 (HSPD-12 Policy Memo) established a requirement for this APL and mandated its government-wide use.

Benefits:

- Certification provides a level of assurance through a validated third-party that adequate proof was provided for each control or capability.

Potential Opportunities for Improvement:

- Strengthened SCRM considerations during the evaluation process.

Ensure that changes to risks in the supply chain ecosystem for FICAM products and services are monitored regularly and that mitigations and other response actions are appropriately planned for and executed.

DOD CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

The Office of the Under Secretary of Defense for Acquisition and Sustainment is working with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers, and industry to develop the Cybersecurity Maturity Model Certification (CMMC). WG3 plans to closely monitor this program as it undergoes initial implementation due to perceived relevance to WG3's objectives.

- The CMMC will review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats.
- The CMMC effort will build upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements.
- The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels.
- The intent is for certified independent third-party organizations to conduct audits and inform risk.

Potential Benefits of the DoD CMMC:

- The evaluation process seeks to provide more maturity with a repeatable process that delivers more consistent results using a data-driven methodology for assessment and scoring.

THE NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA) SOLUTIONS FOR ENTERPRISE-WIDE PROCUREMENT (SEWP)

NASA SEWP is a multi-award suite of contracts managed by the NASA SEWP PMO and serves as an information channel between industry and government as well as between agency decision makers and their acquisition teams. The office mediates actions between industry and government, facilitates the acquisition process, and recommends best approaches to acquisition issues (SEWP is currently used by every government agency). The SEWP contract rate is among the lowest fee structure for similar contract vehicles and features a responsive customer service-oriented structure.

There are several SCRM standards and guidelines, including NIST Special Publication 800-16 Supply Chain Risk Management Practices for Federal Information Systems and Organizations, and the Open Trusted Technology Provider Standard (O-TTPS). The O-TTP is industry led with the DoD and NASA participation and assists customers with identifying COTS technology. The O-TTPS standard is a set of prescriptive requirements and recommendations for organizational best practices regarding

technology development and supply chain activities. Technology providers and government collaborate to establish *best of breed* best practices to create a standard that enables providers to build trustworthy products; additionally, the Open Group's Trusted Technology Forum (OTTF) has created an accreditation program that identifies trusted technology providers who meet this standard. These practices enhance the security and integrity of COTS ICT and help secure global supply chains from threats.

There are also a number of critical SCRM issues which are addressed by the implementation of standards. Although 100% assurance is impossible, risk can be identified and assessed. Using authorized resellers can have a negative effect on small businesses by reducing competition. It is also important to note that decision making regarding the success or failure of a reseller is completely at the discretion of the manufacturer and can be subjective. Letters of authorization may be provided and reduce risk, but are often not as reliable as official SEWP verification.

Additionally, specific resellers and distributors can be authorized. An authorized reseller is a defined program or process that often requires technical knowledge and funds. More specifically, established authorized resellers can be utilized when reseller or provider relationships are most critical. Established authorized resellers must meet specific criteria and provide a documented process and point of contact who can verify the trustworthiness of these resellers.

Appendix D: Examples of QLs and Program Activities

EXAMPLE	DESCRIPTION
State of Virginia Department of Transportation (VDOT) Material Approved List https://www.virginiadot.org/business/resources/Materials/ApprovedLists/Materials_Approved_Lists.pdf	Provides a list of products; where to source them (manufacturer), and evidence for last tests. (Many states have similar Approved Products Lists)
DoD Information Network (DoDIN) APL Testing and Certification https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/dod-information-network-dodin-apl-testing-and-certification	The DoD Information Network Approved Products List (DoDIN APL) is established in accordance with the UC Requirements (UCR 2013) document and mandated by the DoD Instruction (DoDI) 8100.04. Its purpose is to maintain a single consolidated list of products that have completed Interoperability (IO) and Cybersecurity certification. Use of the DoDIN APL allows DoD components to purchase and operate systems over all DoD network infrastructures. The DoDIN APL is the only listing of equipment by DoD to be fielded in DoD networks. DoD components are required to fulfill their system needs by only purchasing DoDIN APL listed products, providing one of the listed products meets their needs. This means the DoDIN APL must be consulted prior to purchasing a system or product. If no listed product meets the organization's needs, they may sponsor a product for testing that does meet their needs.
GSA ID-Management APL https://www.idmanagement.gov/approved-products-list/	The APL provides federal agencies with products and services that have been approved for FICAM implementation based on rigorous security vulnerability and interoperability testing performed by the FIPS 201 Evaluation Program.
DoDIN Approved Products List https://aplits.disa.mil/processAPList.action https://aplits.disa.mil/docs/aplprocessguide.pdf	The DoD Information Network (DoDIN) APL is the single consolidated list of products that have completed IO and Cybersecurity certification. The DoDIN APL process is used to test and certify products that affect communication and collaboration across the DoDIN and is an acquisition decision support tool for DoD organizations interested in procuring equipment to add to the Defense Information System Network to support their mission. The DoD 8100.04 policy and Unified Capabilities Requirements (UCR) 2013 Change 2 define the scope of the DoDIN APL. The DoDIN APL Process Guide provides guidance on the step-by-step process from submission to placement on the DoDIN APL. It also includes a description of the process to maintain the DoDIN APL and roles and responsibilities of participants in the process.

GSA-list of Continuous Diagnostics and Mitigation (CDM) Program (tools/capabilities) https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm-program	The CDM program helps strengthen the cybersecurity of government networks and systems. CDM provides federal agencies with capabilities and tools that find cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to focus on the most significant problems first. For CDM Tools SIN 132-44 (legacy) / 541519CDM (new) Information for Ordering Organizations.
National Information Assurance Partnership (NIAP) https://www.niap-ccevs.org/Ref/What_is_NIAP.CCEVS.cfm https://www.niap-ccevs.org/Product/	"NIAP oversees a national program to evaluate COTS IT products for conformance to the International Common Criteria. This program includes the NIAP-managed Common Criteria Evaluation and Validation Scheme (CCEVS or Scheme), a national program for developing protection profiles, evaluation methodologies, and policies that ensures achievable, repeatable, and testable security requirements. The CCEVS is a partnership between the public and private sectors to provide COTS IT products that meet consumer needs and to help manufacturers of those products gain acceptance in the global marketplace. Successful evaluations benefit industry product developers/vendors and government procurers by validating that the products meet security requirements for U.S. national security system procurement. Because NIAP is a member of the international 31-nation Common Criteria Recognition Arrangement (CCRA), NIAP-validated products are also available to procurers in the CCRA member nations. IT security testing is conducted by NIST-accredited and NIAP-approved commercial testing labs. A product vendor chooses an approved lab to complete the product evaluation against a selected applicable protection profile. A protection profile is an implementation-independent set of security requirements for a particular technology that enables achievable, repeatable, and testable evaluation activities for each evaluation. All products evaluated within the Scheme must demonstrate exact compliance to the applicable technology protection profile. NIAP assesses the results of the security evaluation conducted by the lab and, if the evaluation is successful, issues a validation certificate and lists the product on the U.S. NIAP Product Compliant List and the international CCRA Certified Products List. U.S. Customers (designated approving authorities, authorizing officials, integrators, etc.) may treat these mutually-recognized evaluation results AS Complying with the Committee on National Security Systems Policy (CNSSP) 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products - dated June 2013 (https://www.cnss.gov/CNSS/issuances/Policies.cfm)."

	"The products listed below must be considered in the context of the environment of use, including appropriate risk analysis and system accreditation requirements. Customers must ensure that the products selected will provide the necessary security functionality for their architecture. The following products, evaluated and granted certificates by NIAP or under CCRA partnering schemes, comply with the requirements of the NIAP program and, where applicable, the requirements of the Federal Information Processing Standard (FIPS) Cryptographic validation program(s). Products on the Product Compliant List (PCL) are evaluated and accredited at licensed/approved evaluation facilities for conformance to the Common Criteria for IT Security Evaluation (ISO Standard 15408). U.S. Customers (designated approving authorities, authorizing officials, integrators, etc.) may treat these mutually-recognized evaluation results AS Complying with the Committee on National Security Systems Policy (CNSSP) 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products - dated June 2013 (https://www.cnss.gov/CNSS/issuances/Policies.cfm). NIAP has implemented the CCRA Management Committee Vision Statement for the application of the CC and the CCRA and no longer evaluates against Evaluation Assurance Levels (EAL). This strengthens evaluations by focusing on technology specific security requirements. The products listed below are evaluated against a NIAP-approved Protection Profile, which encompasses the security requirements and test activities suitable across the technology with no EAL assigned—hence the conformance claim is "PP". NIAP Lists can be searched and sorted by company/organizations and products/technologies.
Penn State University (PSU) list of pre-approved road construction materials https://www.dirtandgravel.psu.edu/sites/default/files/PA%20Program%20Resources/Products/Approved_Products_List.pdf	"The Dirt and Gravel Road Maintenance Program was founded on solid environmental principles. One of these principles is the program's strict limitations on the use of products that may cause damage to the environment in any way. Listed here are the products approved for purchase and use with program funding. The program does not endorse these or any other individual products."
Food and Drug Administration's (FDA) Approved Drugs https://www.accessdata.fda.gov/scripts/cder/daf/	Drugs@FDA includes information about drugs, including biological products, approved for human use in the U.S. (see FAQ), but does not include information about FDA-approved products regulated by the Center for Biologics Evaluation and Research (for example, vaccines, allergenic products, blood and blood products, plasma derivatives, cellular and gene therapy products). For prescription brand-name drugs, Drugs@FDA typically includes the most recent labeling approved by the FDA (for example, Prescribing Information and FDA-approved patient labeling when available), regulatory

	information, and FDA staff reviews that evaluate the safety and effectiveness of the drug.
Example of a Standard used for Evaluation against a Qualification Requirement (E.g., Qualification Criteria: Bidder shall have an effective quality assurance program in place. Standard for Evaluation: ISO-9000 or equivalent; Qualification Evidence: Certification) https://en.wikipedia.org/wiki/ISO_9000	Can be called out as a specific certification as a pre-requisite to qualify for bid. For example: ISO-9000 Quality Assurance Certified / ISO-9000 certified / compliant. "The ISO 9000 family of Quality Management Systems (QMS) is a set of standards that helps organizations ensure they meet customers and other stakeholder needs within statutory and regulatory requirements related to a product or service.[1] ISO 9000 deals with the fundamentals of quality management systems,[2] including the seven quality management principles that underlie the family of standards.[2][3][4] ISO 9001 deals with the requirements that organizations wishing to meet the standard must fulfil.[5] Third-party certification bodies provide independent confirmation that organizations meet the requirements of ISO 9001. Over one million organizations worldwide [6] are independently certified, making ISO 9001 one of the most widely used management tools in the world today. However, the ISO certification process has been criticized [7][8] as being wasteful and not being useful for all organizations."
Part 9 - Contractor Qualifications FAR Acquisition.GOV https://www.acquisition.gov/far/part-9	This part prescribes policies, standards, and procedures pertaining to prospective contractors' responsibility; debarment, suspension, and ineligibility; qualified products; first article testing and approval; contractor team arrangements; defense production pools and research and development pools; and organizational conflicts of interest.
European Space Agency ESCC Qualified Manufacturers List https://escies.org/webdocument/showArticle?id=727	This a list of qualified manufacturers that have been certified by the European Space Agency for technology flows to the rules of the ESCC system with principle reference to ESCC Basic Specification no. 25400. The qualified electronic components produced from the technology flows are intended for use in ESA and other spacecraft and associated equipment in accordance with the requirements of the ECSS standard ECSS-Q-ST-60. Each technology flow qualification and its subsequent maintenance is monitored and overseen by the ESCC executive. ESA certifies the qualification upon receipt of a formal application from the executive stating that all applicable ESCC requirements have been met by the pertinent manufacturer. The qualified status of a technology flow is noted by an entry in this document, a corresponding entry in the European space components information exchange system, ESCIES, and the issue of a certificate to the qualified manufacturer.

Appendix E: Hardware Integrity Resources

The following are resources identified by WG3 that will assist users of this report to incorporate hardware integrity and security into criteria for QLs.

> "Tamper-resistance: The world of FIPS 140-2 certified cryptographic hardware has a similar requirement at levels 2 and 3. Devices certified to FIPS 140-2 Level 2 are required to "show evidence of tampering", which is usually accomplished by putting stickers similar to the usual "Warranty-void if removed" type stickers over screw holes and seams, but the FIPS 140-2 version of these stickers are serial numbered and like explode ink and change colours when you remove them. They are not fool-proof though and can be removed with a lot of skill and patience. Devices certified to FIPS 140-2 Level 3 are required to have "strong enclosures and tamper-detection/response circuitry that zeroes all [cryptographic keys] when the removable covers/doors of the [device] are opened." "You tend to see this on high end servers intended for performing cryptography (i.e., HSMs) which run in the $1,000 - $10,000 USD range. You never see this kind of tamper-evidence/tamper-resistance on consumer devices like hard disk drives and keyboards, but they could be developed if there is a market for it?"
>
> "Hardware fingerprinting: Physically Unclonable Functions (PUFs)… are essentially hardware hash functions in the sense that they will always give the same output to the same input, but their behavior is very hard to characterize or duplicate. These are usually complex crystals where you measure a laser's optical path, or complex electrical circuits where you measure precise latency and resistance from input pins to output pins. They are mainly used for uniqueness -- each device has a unique fingerprint – but their signature will change after physical tampering (I've heard of PUFs being built into device casings to detect if the seal has been broken, for example).
>
> Bottom-line: We do not have (full)… "tamper-resistance …for consumer devices. In theory it's possible, but would probably significantly increase the cost of the device. A reasonable middle-ground for the amateur …is to only buy electronics in-person off the shelf from reputable big-box stores, and never order them online where they will be shipped across the country (and possibly across international borders) with your name on the box."… or leverage USG / DoD "blind-buy process."[14]

Additional standards and controls that may be leveraged include, but are not limited to:

1. "…Federal Information Processing Standards (FIPS) -140 compliant devices, which at module and chip level may implement tamper evidence/resistance. Often this is done with high-integration (holding the security system in silicon) and strong physical shielding, e.g., via hardened casings, epoxy resin covered components or modules, thin wires shielding sensitive areas; or methods at chip level (mechanisms in silicon and wiring layers, such as X-Ray protection or fuddling metal layers), such as known from integrated circuit card (ICC) products and other security hardware. In addition, hardware security module (HSM) modules are designed to protect themselves, but not to protect an external system or element.

   Hence, the problem may arise that active tamper evidence and/or detection mechanisms are missing, which enable either self-protection of a system against physical attacks or provide means to remotely detect such tampering events. Hence, there may be a need to provide for (additional) hardware integrity protection."[15]
2. NIST SP 800-53's "SA-10 (3) Hardware Integrity Verification: This control enhancement allows organizations to detect unauthorized changes to hardware components through the use of tools, techniques, and/or mechanisms provided by developers. Organizations verify the integrity of hardware components, for example, with hard-to-copy labels and verifiable serial numbers provided by developers, and by requiring the implementation of anti-tamper technologies. Delivered hardware components also include updates to such components.

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of hardware components."[16]

3. ISO/IEC 27036 includes HWA requirements content. "ISO/IEC 27036-2:2014 specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships.

   These requirements cover any procurement and supply of products and services, such as manufacturing or assembly, business process procurement, software and hardware components, knowledge process procurement, Build-Operate-Transfer and cloud computing services.

   These requirements are intended to be applicable to all organizations, regardless of type, size and nature.

   To meet these requirements, an organization should have already internally implemented a number of foundational processes or be actively planning to do so. These processes include, but are not limited to the following: governance, business management, risk management, operational and human resources management, and information security."[17]

4. NIST Special Publication 800-160 VOLUME 1 Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems https://adventuresinsecurity.com/Files/NIST_SP_800_160_v1.pdf

5. ISO/IEC/IEEE 15288, Systems and software engineering — Systems life cycle processes. https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:15288:ed-1:v1:en

6. ISO/IEC 15026, Systems and software engineering -- Systems and software assurance https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:15026:-1:ed-1:v1:en

7. There is a robust effort to develop a holistic approach to Information Systems Security partially captured here (on implementing the ISO/IEC 270xx series/family of standards: https://www.ogcio.gov.hk/en/our_work/information_cyber_security/collaboration/doc/overview_of_iso_27000_family.pdf

There is an acute need for this holistic approach to C-SCRM that includes hardware assurance or integrity.

Following is a representative list of other successful efforts in hardware integrity assurance, that are not specifically standards:

- Trusted Foundry Program: www.trustedfoundryprogram.org.
- The Trust in IC program: started by the DARPA in 2007 to develop efficient methods for Hardware Trojan detection.
- DARPA's Supply Chain Hardware Integrity for Electronics Defense (SHIELD/dielets).
- The ENISA (European Networks and Information Security Agency) effort initiated in 2011 towards securing the Supply Chains of electronics security devices.

Following are emerging and ongoing efforts relevant to hardware integrity:

Accellera.org is evaluating and improving "IEEE 1685, "Standard for IP-XACT, Standard Structure for Packaging, Integrating and Re-Using IP Within Tool-Flows," describes an XML Schema for meta-data documenting Intellectual Property (IP) used in the development, implementation and verification of electronic systems and an Application Programming Interface (API) to provide tool access to the meta-data. This schema provides a standard method to document IP that is compatible with automated integration techniques. The API provides a standard method for linking tools into a

system development framework, enabling a more flexible, optimized development environment. Tools compliant with this standard will be able to interpret, configure, integrate and manipulate IP blocks that comply with the proposed IP meta-data description. The standard will be independent of any specific design process. It does not cover the behavioral characteristics of the IP."[18]

SAE G32: The SAE G-32 Cyber Physical Systems Security (CPSS) Committee and all subcommittees will develop and maintain technical documents (Standards, Handbooks, Recommended Practices and Information Reports) to further CPSS including analyses of the system operating environment defined by the operational, functional, and architectural systems engineering elements. Through the G-32, this committee is chartered under the SAE Aerospace Council's authority and its documents are intended for broad industry use (commercial, defense, and other high reliability and/or critical systems in aerospace, transportation, medical, etc.). G32 has a specific Working Group on Hardware Assurance (HwA).

Hardware Assurance Body of Knowledge (HwA BoK): The Office of the Undersecretary of Defense for Research and Engineering has funded Institute of Defense Analysis (IDA) to lead a HwA BoK effort (in 2020) to support Systems Security Engineering and the Systems Engineering SEBoK. https://www.sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_(SEBoK).

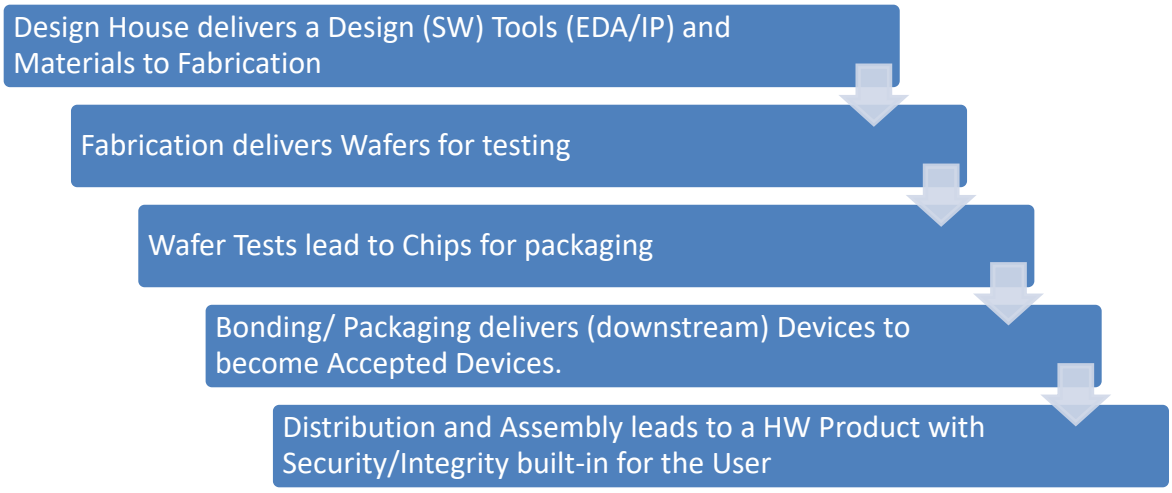
Some Mitigation Efforts in Hardware Integrity are explained here:

https://hal-cea.archives-ouvertes.fr/cea-01094255/file/Fournier_2013_Hardware%20integrity_LETI_Innov_Days.pdf

Mitigation topics, listed below:

- Approach to mitigation selection [full life cycle]
- How to select appropriate mitigations in the context of the overall architecture
- Show importance of linking across life cycle and up/down stack
- Refocus to hardware subsegment in that context
- Applying mitigations to risk profiles
- How are specific mitigations to specific risk profiles applied in practice
- Mention interplay of mitigations between lifecycle levels
- Refocus and expound upon hardware subsegment in that context
- Defense in-depth [maximal protection] balanced with cost/need
- Example mitigations for specific identified risks
- Evolve over time, flexibility in approach and method are required
- Risk profile changes over time
- Engineering choices and assumptions driving risk increases over time
- Pick commonly known risks and present the mitigations applied, when, how
- Overall methodology to ensure flexibility and risk minimization in context
- One-time protections vs. reconfigurable protections
- Utility of 'Mitigation in depth' approaches to mitigate for future risk profile changes
- Overall methodology to apply flexible methods and risk minimization over time

A very simplistic lifecycle view of integrated circuits and microchips (below) shows us where we have to document data collected for decisions to progress. HWI-data needs to better influence these lifecycle decisions/progressions.



Below are some areas of influence (potential risk mitigations) that can be used in the decisions/progressions above:

- 'Cryptographic' activation of chip or restricting access to some parts of the chip,
- Visual inspection,
- Puf-based authentication,
- Obfuscation,
- Watermarking, and
- Dynamic encryption of bit streams (for FPGAs, blurring hardware/software (HW/SW) lines.

Additional examination of lifecycle processes, products, risk acceptance decisions might include:

- Full Electronic Design Automation (EDA) tools for foundry and ASIC flows; extendable to other State of the Art (SOTA) nodes;
- Accreditation to handle classified, controlled-unclassified information (CUI), ITAR/EAR data, and other controlled data or information;
- Full data assurance of the design via secure release to accredited mask house companies for "mask root of trust";
- Foundry model using continuous monitoring and manufacturing control system insights to provide full traceability, including preventing "excursions," recovering all scrap and segregation of material for protection;
- Post-production controls, including logistics monitoring and integration into special services such as packaging and test;
- Controlled shipping to sensitive client locations globally;
- Return material authorization (RMA) management and long-term storage for "respins" of programs for extending lifecycle beyond normal commercial standards; and
- Insider threat prevention via best security practices and program controls along with close coordination with government clearance authorities.

Following are some additional design for security areas and a few representative examples:

1. HW/SW Tags: Counterfeiting, design security, obfuscation, reverse engineering, side-channel analysis. Although a recognized if imperfectly executed issue in software, design for security is an emerging topic in hardware engineering, reaching way beyond the precautions taken during the creation of cryptographic and other supposedly secure blocks in system-on-chip (SoC) development.

Disaggregated manufacturing and supply chains, the rise of cyber-physical systems and the internet of things (IoT) as well as the near universal use of third-party IP cores in SoCs—now numbering more than 100 individual cores on ICs implemented on advanced nodes—has given rise to concerns over the security not just of the software they execute but the hardware as well. Much of the existing secure-software infrastructure, which relies on concepts such as the root of trust and a secure-boot sequence relies on the assumption that the underlying hardware has not been compromised by an attacker. If the hardware is compromised, the rest of the system is vulnerable.[19]

2. Acquirers should demand suppliers provide them information on the hardware (and software) included in products they are consuming/building into their enterprise. There may be a need for a HW Bill-of-Materials (BOM) similar to the Department of Commerce National Telecommunications and Information Administration (NTIA) efforts in (SW) SBOM.[20]

3. A good overall general example of that type of information is covered by ISO/IEC 20243, which is derived from the Open Group's O-TTPS.

   ISO/IEC 20243-1:2018 (O-TTPS) is a set of guidelines, requirements, and recommendations that address specific threats to the integrity of hardware and software COTS ICT products throughout the product life cycle. This release of the standard addresses threats related to maliciously tainted and counterfeit products.

   The provider's product life cycle includes the work it does designing and developing products, as well as the supply chain aspects of that life cycle, collectively extending through the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal. While this standard cannot fully address threats that originate wholly outside any span of control of the provider—for example, a counterfeiter producing a fake printed circuit board assembly that has no original linkage to the Original Equipment Manufacturer (OEM)—the practices detailed in this standard will provide some level of mitigation. An example of such a practice would be the use of security labeling techniques in legitimate products.

   The O-TTPS stands for "Open Trusted Technology Provider Standard." It is an open standard containing a set of organizational guidelines, requirements, and recommendations for component suppliers, providers, and integrators to enhance the integrity of COTS ICT products and the security of the global supply chain. O-TTPS Version 1.1 – Mitigating Maliciously Tainted and Counterfeit Products, if properly adhered to, will help assure against the threat of tainted and counterfeit products throughout the COTS ICT product lifecycle encompassing the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal.

4. NIST is developing HW security guidelines:

   "Cyber supply chain risks may include unauthorized production, tampering, theft, and insertion of unexpected software and hardware, as well as poor manufacturing and development practices in the cyber supply chain. Tampering or misconfiguration in an organization's supply chain is a difficult challenge to effectively solve. Modern supply chains are highly complex, introducing risk of tampering at numerous points," the draft guidance from NIST states.

   One of the main challenges with supply chain security is the sheer number of parties involved in any one particular device's manufacture, distribution, and sale. A given laptop or server could have major components from a dozen or more separate suppliers, and each of those components may comprise parts from several other individual suppliers. All of those components are then assembled by the OEM and either sold directly to the end customer or through a channel partner or other distributor. Each link in that chain represents a potential

risk for tampering, and the customer virtually never has any visibility into the practices of the various companies involved, so IT departments essentially have to trust that the hardware they're buying is genuine and unadulterated.

The NIST draft guidelines include a few different potential methods for verifying to a reasonable degree that the hardware is what it's billed as and hasn't been altered. The proposed methods rely mainly on some attribute that is irrevocably bound to the hardware and can be verified by the end customer, such as a serial number or other identifier. One potential drawback of this approach, though, is that it relies on the enterprise IT team to perform some testing of a given piece of hardware, which can be complex and difficult.

"This project will leverage verifiable and authentic artifacts that manufacturers produce during the manufacturing and integration process that can support C-SCRM. This may include manufacturer declarations of platform attributes (e.g., serial number, list of hardware components) and measurements (e.g., firmware hashes) that are tightly bound to the hardware itself. For example, these declarations of attributes and measurements could be cryptographically linked to a strong device identity, such as those associated with the Trusted Platform Module (TPM) or Device Identifier Composition Engine," the draft guidance from NIST says.[21]

Lessons Learned from a Public Private Partnership specifically focused on HWA/HWI:

National Defense Industrial Association (NDIA) Trusted Microelectronics Joint Working Group (TM JWG) enables government and industry to jointly address critical dependencies between microelectronics components, systems security and information assurance. The working group has been helping DoD and civilian agencies develop methods of acquiring trusted and trustable microelectronics, printed circuit boards, and other electronic components for Defense and security systems from a market that is now dominated by commercial buyers and foreign sources.[22]

In 2017, the working group self-organized into four teams, addressing:

1. Future Needs and System Impact of Microelectronics Technologies,
2. Trustable Access to Leading Edge Technology,
3. Trustable Microelectronics Standard Products, and
4. New Methods to Instill Trust in Commercial Semiconductor Fabrication.

Summary of Findings and Recommendations:

"There are tremendous upsides with using commercial microelectronics. For example, defense systems can be afforded highly advanced components such as FPGAs, memory chips or receiver chips that might have cost over $100 million to develop and bring to market, but sell for a small fraction of the development cost from amortizing that cost across the commercial applications' volume manufacturing. Catalog chips that are in wide use would conceivably be subject to global security challenges and evaluations with corporate documentation of errata or issues of fixes addressed via firmware updates etc., thus improving the component's reliability over time. On the downside, using commercial components coupled with long-lived defense systems can create long-term obsolescence problems for defense systems as the life-cycle of chip technologies becomes shorter and shorter.

From a security perspective, a commercial component might be susceptible to an unpublicized vulnerability for an adversary to exploit if enough effort were spent examining the chip. It is possible for a custom or semi-custom chip to have an analogous flaw, but if it were produced using a trusted flow it is presumed to be difficult for an adversary to obtain the chip and the design information needed to exploit the flaw."

The NDIA TM JWG Team 3 on Trustable Microelectronics Standard Products recommends that DoD and others:

- Develop and employ a consensus approach for establishing categories of trustworthiness for catalog chips based on risks, commercial practices, use of standards (SAE, ISO or Open Group accreditation procedures etc.) or quantifiable supplementary information that can be supplied with respect to a catalog chip. This approach should lead directly to a methodology for assessing individual microelectronics used in critical roles in defense systems. Using a categorization approach to establish various levels and mitigations will require expert inputs and debates, but will provide the best long-term solution for DoD, the U.S. government (USG), and U.S. critical infrastructure.
- Partner with non-defense industries working with commercial microelectronics companies to enhance security status and affordability of catalog chips in areas like industrial standards and supply chain practice.
- With vendor participation, the Defense Microelectronics Industry (DMEA) Category II criteria could be used for an additional level of trust above the basic best commercial practice.

The overall key recommendations from all four teams:

- Create a U.S. National Semiconductor Strategy: The absence of a comprehensive national semiconductor strategy was viewed by the TM JWG as a major impediment to assuring access to critical national security technologies and to U.S. technological competitiveness.
- Adapt DoD Acquisition Practices to Align with Commercial Market: The TM JWG's analyses highlight the differences between DoD's acquisition practices and commercial sales priorities. The TM JWG recommends defense programs be provided new methods to purchase technology on commercial terms after the commercial products have been evaluated for trustworthiness.
- Increase DoD Market Influence: The DoD's share of the semiconductor market has dramatically declined to less than 1% of today's semiconductors consumption, and the Department's ability to gain access to needed microelectronics capabilities has correspondingly diminished. The TM JWG suggests actions that can increase market influence by exchanging research investment for access to commercial products; and, aggregating demand across DoD programs, other USG offices, and non-USG industries that have similar component and system integrity concerns.
- Adopt New Trust and Assurance Models: The JWG's analyses articulated the value of developing program-specific trust plans and technical implementation guides to identify security measures for each step in the product flow from design through test. The guides would factor technology-enabled mitigations and countermeasures into security requirements; the plans could expand today's trust offerings by defining the boundaries for assurance spectrums or tiers of trust levels, and would cover component categories beyond ASICs.

Launch Research and Development to Achieve Trust / Security in Un-trusted

Separate from, but coordinated with, the national semiconductor strategic plan, the TM JWG recommends launching near-term research and development to address the security concerns of existing commercial technology capabilities, including Trusted 3D/2.5D integration, to leverage these capabilities for defense systems. Establishing a government focus to track future technology trends and impacts is recommended to continuously identify technology renewal opportunities and capabilities gaps.

EXAMPLE OF USE OF STANDARDS TO ADDRESS HARDWARE SECURITY

Only users/capability-owners can really drive effective risk mitigations, because they best understand their mission, function/capability and system risk tolerance: ISO/IEC 26262[23] is an example of this type of effort.

The automotive industry (developers) and user community developed a sector/product specific functional safety/security standard, leveraging quality and safety work. ISO/IEC 26262 is a standard related to the safety of electrical and electronic systems within a car and addresses possible hazards caused by malfunctioning behavior of safety-related systems, including interaction of these systems.

Appendix F: References

CDM Tools SIN, V. (2019). *CDM SIN Information for Vendors.* Retrieved from CDM SIN Information for Vendors: https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm/continuous-diagnostics-mitigation-cdm-tools-special-item-number-sin-information-for-vendors

CDM Tools SIN, G. (2019). *CDM Tools SIN.* Retrieved from Continuous Diagnostics and Mitigation (CDM) Program: https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm-program

C-SCRM. (2019, August 03). *CISA*. Retrieved from Cyber Supply Chain Risk Management: https://www.cisa.gov/supply-chain

FAR 9.104.2. (n.d.). *Federal Acquisition Regulation (FAR).* Retrieved from 9.104.2 - Special Standard: http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/09.htm

HSSEDI. (2019, January 28). *ICT SCRM TF.* Retrieved from Preliminary Statement of Goals, Objectives, Operations, Activities, Plans, and Milestones.

ICT SCRM TF, C. (2018, December 13). *Charter for the ICT SCRM TF.* Retrieved from Charter for the ICT SCRM TF.

IDManagement, G. (2019). *FIPS 201 Approved Products List.* Retrieved from https://www.idmanagement.gov/approved-products-list/

IT Schedule 70, G. (2019). *IT Schedule 70, .* Retrieved from IT Schedule 70, : https://www.gsa.gov/technology/technology-purchasing-programs/it-schedule-70

Monette, E. (2018, October 16). *Memorandum for ICT SCRM TASK FORCE.* Retrieved from Memorandum for ICT SCRM TASK FORCE.

News Press Release, C. (2018, October 30). *DHS and Private Sector Partners Establish Information and Communications Technology Supply Chain Risk Management Task Force.* Retrieved from DHS and Private Sector Partners Establish Information and Communications Technology Supply Chain Risk Management Task Force: https://www.cisa.gov/news/2018/10/30/dhs-and-private-sector-partners-establish-information-and-communications-technology

News Press Release, C. (2018, November 15). *DHS Announces ICT Supply Chain Risk Management Task Force Members.* Retrieved from DHS Announces ICT Supply Chain Risk Management Task Force Members: https://www.cisa.gov/news/2018/11/15/dhs-announces-ict-supply-chain-risk-management-task-force-members

News Press Release, C. (2019, February 26). *CISA's ICT Supply Chain Risk Management Task Force Launches Work Streams.* Retrieved from CISA's ICT Supply Chain Risk Management Task Force .Launches Work Streams: https://www.cisa.gov/news/2019/02/26/cisa-s-ict-supply-chain-risk-management-task-force-launches-work-streams

NRMC. (2018, November 15). *CISA.* Retrieved from National Risk Management Center: https://www.cisa.gov/publication/information-and-communications-technology-supply-chain-risk-management-task-force

[1] See, 48 CFR 9.201, 9.203(a) (2020).

[2] NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, available at https://csrc.nist.gov/publications/detail/sp/800-161/final.
[3] https://www.cbp.gov/sites/default/files/documents/3pl_security_criteria_3.pdf
[4] See, https://www.cisa.gov/critical-infrastructure-sectors
[5] See, e.g., https://www.nist.gov/system/files/documents/2017/05/18/financial_services_csf.pdf and https://www.energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf
[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf
[7] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[8]https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
[9] https://csrc.nist.gov/publications/detail/white-paper/2020/04/23/mitigating-risk-of-software-vulnerabilities-with-ssdf/final
[10] https://www.bsa.org/files/reports/bsa_software_security_framework_web_final.pdf
[11] https://safecode.org/wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf
[12] See FAR Part 9.202
[13] https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8276-draft.pdf
[14] https://security.stackexchange.com/questions/191422/how-to-check-hardware-integrity
[15] https://patents.google.com/patent/EP2950233A1/en
[16] https://www.stigviewer.com/controls/800-53/SA-10
[17] https://www.iso.org/standard/59680.html
[18] https://www.accellera.org/activities/working-groups/ip-xact
[19] https://www.techdesignforums.com/practice/guides/design-security/
[20] https://www.ntia.gov/files/ntia/publications/framingsbom_20191112.pdf
[21] https://duo.com/decipher/nist-developing-hardware-security-guidelines-for-enterprises
[22] https://www.ndia.org/divisions/working-groups/tmejwg
[23] https://semiengineering.com/knowledge_centers/automotive/iso-26262/