DoD CIO
C-SCRM Risk Assessment for Procurement Types

DCIO/CS Risk Assessment & Operational Integration

AEROSPACE REPORT NO.
TOR-2020-02651

C-SCRM Risk Assessment for Procurement Types

February 7, 2022

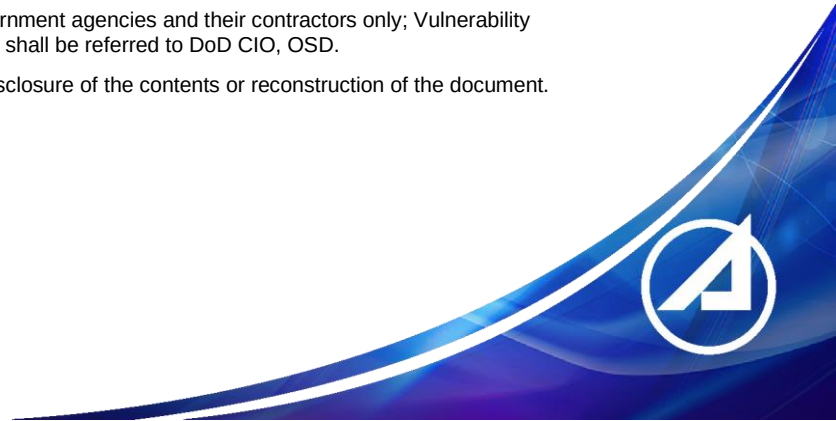
Paul de Naray
OSD Analysis
National Space Systems Engineering

Prepared for:

DoD CIO - Risk Assessment & Operational Integration
6000 Defense Pentagon
Washington, D.C. 20301

Contract No. FA8802-14-C-0001

Authorized by: Defense Systems Group



Foreword

This document was authored to assist government organizations with understanding how to manage risk from the supply chain during their procurement. The structure is built off a series of procurement types that have increasing resources for risk management. The practices described are built upon Department of Defense (DoD) Instruction 5000.90 [1] for cybersecurity in the supply chain and are informed by the author's experience with cybersecurity risk in supply chain risk management across the DoD. While this document focuses on a series of procurement types utilized by DoD, if an organization would like to follow a hierarchical, enterprise perspective for organization of supply chain risk management, then the reader should consult NIST Special Publication (SP) 800-161 [2]. This document is driven by DoD Chief Information Officer (CIO) efforts to communicate best practices and considerations across DoD as organizations define or refine risk assessment for their supply chains.

Contents

1. Procurement Types 4

2. Risk Tolerance and C-SCRM Analysis Resources 4

3. Risk Assessment & Mitigations 7
   - 3.1 Simplified Procurement Best Practices 8
     - 3.1.1 Risk and Response 9
   - 3.2 Structured Procurement Best Practices 9
     - 3.2.1 Threats and Vulnerabilities 10
     - 3.2.2 Risk and Response 11
   - 3.3 Engineered and Assured Procurement Best Practices 11
     - 3.3.1 Mission Impact through Criticality Analysis 12
     - 3.3.2 Threats and Vulnerabilities 15
     - 3.3.3 Risk and Response 15

Figures

Figure 1 - Risk Tolerance 4
Figure 2 - Procurement Type Risk Tolerance vs SCRM Analysis Resources 5
Figure 3 - Main risk components 7
Figure 4 - Basic Risk Assessment Process 8
Figure 5 - Simplified Procurement Focus on Externally Provided Risk Assessments 8
Figure 6 - Structured Procurement Ability to Assess Threat and Vulnerability 10
Figure 7 - Engineered Procurement Full Risk Assessment and Responses 12
Figure 8 - Decomposition of Mission Impact Through Criticality Analysis 12

Tables

Table 1 - Example CPI Impact Criteria 14

1. Procurement Types

Acquiring military components and supplies can range from commodity commercial products procured through basic purchase cards, to complex Major Capability Acquisitions defined in DoDI 5000.02 "Operation of the Adaptive Acquisition Framework". This range of procurement can have significantly different requirements and expectations on the actions necessary to manage system risk from the supply chain risk.

For the purposes of this document, the range of procurements types are separated into four levels reflecting increasing complexity: Simplified, Structured, Engineered, and Assured.

- **Simplified** – Micro-purchase of components the sum of which cannot exceed a set cost threshold (e.g., $10,000). Examples include ad-hoc computer components or ad-hoc software procured with a purchase card.
- **Structured** – Automated procurement of high-demand, commodity component purchases. This procurement reduces uncertainties in product choices and controls transaction costs associated with supplier search, approvals, processing, and ordering. Examples include wireless network components, enterprise software, and commercial service providers.
- **Engineered** – Custom engineering services that integrate components into a system capability. This is for more complex or initially uncertain solutions that require engineering support to develop and sustain the system. This work could fall under a DoDI 5000.02 [3] acquisition program (e.g. an ACAT II or III program) and Adaptive Acquisition Framework pathways such as Middle Tier of Acquisition, Urgent Capability Acquisition, Defense Business Systems, Acquisition of Services, or Software Acquisition. Specific examples include an industrial control system in an Abrams tank or a DevSecOps pipeline service.
- **Assured** – Custom engineered system capability like Engineered procurement, but for complex and high consequence systems (e.g., weapon systems). These procurements typically fall under a major DoDI 5000.02 acquisition program such as an ACAT I, but could be any program category or acquisition path with a high consequence and requires assured procurement. Examples include a nuclear command and control, missile warning, and battle management system.

These procurement types serve as a structure for the subsequent cyber supply chain risk management best practices.

2. Risk Tolerance and C-SCRM Analysis Resources

The risk tolerance concept is a threshold of risk impact and likelihood where an organization will make decisions to either accept the risk or perform a risk management response to avoid, transfer, or mitigate the risk. If a risk is below the tolerance level, then the risk is accepted, and no actions are taken besides the tracking and acknowledgment of the risk. For risk above the tolerance threshold, there are management responses that include avoiding the supplier or component altogether (e.g., not purchasing), transfer of the risk to another owner (e.g., user assumes and manages risk), or risk mitigation through tailored actions that lower the risk likelihood or impact. No matter which procurement type

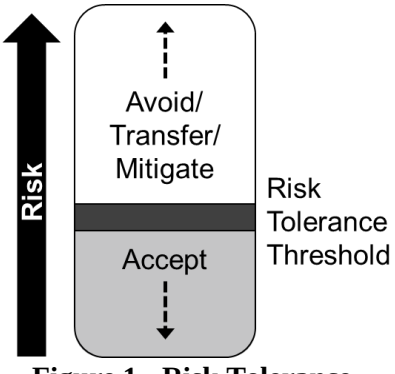


Figure 1 - Risk Tolerance

occurs, an organization must define risk tolerance and assess risk to guide risk responses during procurement.

For any procurement that considers cybersecurity-related supply chain assurance, an assessment must be performed about the risk associated with acquiring a maliciously compromised component. The compromise could be to the component's ability to handle confidential information, integrity of the component's functions, or the component's availability to perform critical functions when needed. Cyber Supply Chain Risk Management (C-SCRM) analysis resources are used during procurement to assess these aspects of confidentiality, integrity, and availability risk associated with the intended use of the component.

The ability to assess supply chain risk requires resources in time, cost, and technical capability. C-SCRM analysis resources are used to identify supply chain information (e.g., gather supplier information, illuminate supplier relationships, collect threat and vulnerability intelligence), to assess risks, and to choose management responses based on the risks and tolerance threshold. C-SCRM analysis resources may be available through enterprise capabilities provided to all within the organization, provided through a specific acquisition effort, or simply left to the resources of the purchaser alone.

Overall, when less C-SCRM analysis resources are available for a procurement, more risk uncertainty will exist due to unknown risk assessments. Risk uncertainty will also create an implicit risk tolerance that matches the maximum amount of risk that could exist within the uncertainty. As previously described, any risk assessed above the risk threshold could be handled via a response to avoid, transfer, or mitigate the risk. This aspect leads to the rationale that as more C-SCRM analysis resources are provided, risk uncertainty will be removed, risks will be assessed and responded to, and ultimately there will be overall lower procurement risk. The combination of these concepts is illustrated in Figure 2.

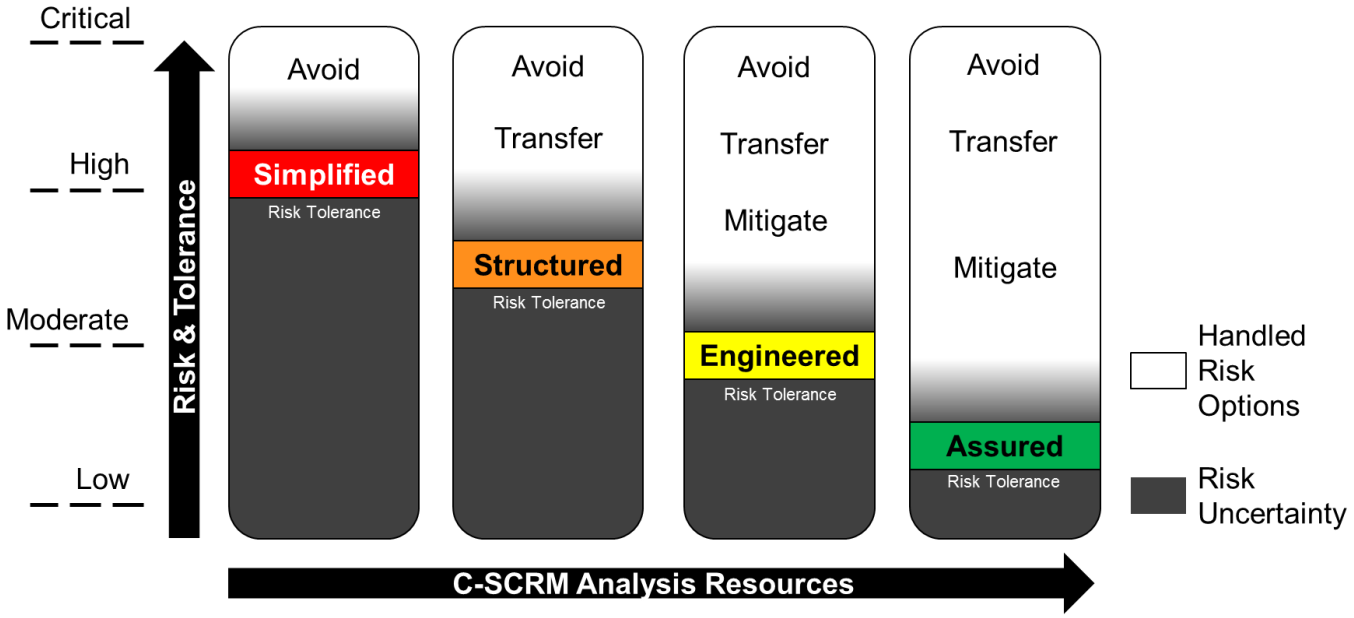


Figure 2 - Procurement Type Risk Tolerance vs SCRM Analysis Resources

The four procurements types are also shown in Figure 2 to depict their general relationship to risk tolerance, C-SCRM analysis resources, and risk assessment uncertainty. While an organization defines its own procurement risk tolerance for supply chain assurance, there are general characteristics associated with procurement types and C-SCRM analysis resources. These general characteristics are not set nor mandated, but rather emerge due to the procurement expectations and resources available.

When C-SCRM risk assessments are determined, any risk management responses will require additional resources to address the risk. The response for avoiding a supplier or component could require little effort as the procurement is simply not made; however, an alternative must still be found to fulfill the procurement need. Resources are required to choose another supplier or component and this effort could be significant if there are limited alternatives available. The transfer response will require minimal resources as the risk responsibility is simply transferred to the end user of the component. The transfer response will still require documentation and communication of the risk assessment to the end user. The mitigation response usually requires the most resources to perform actions that lower risk likelihood or impact. Mitigation responses require active changes such as how the component is used, additional development to protect the system from the component risk, diversification of components to minimize potential risk, or other less intrusive measures.

As shown in Figure 2 procurement types have the following characteristics, which are further explained below.

- **Simplified** – Micro-Purchases of components generally occur on an ad-hoc basis under a blanket approval with little C-SCRM analysis resources available for such a basic purchase effort. Therefore, with few or no resources available for risk assessment there will be a large amount of uncertainty in the procurement risk. This translates to a default risk tolerance threshold no less than high risk. The uncertainty does not likely reach critical risk level due to government enterprise risk assessments and mitigation efforts that avoid critical risk suppliers and components. These risk assessments include decisions under Section 2339a of Title 10 United States Code or Committee on Foreign Investment in the United States (CFIUS) coordination. Government-wide bans of these procurements (i.e., avoidance) should effectively remove critical risks in simplified procurements.
- **Structured** – The procurement of high-demand, commodity purchased components will have overall resources available to manage the automated procurement capability. However, these resources will primarily be dedicated to procurement management and efficient commodity purchases. There will likely be limited C-SCRM analysis resources available for risk assessments. Any C-SCRM analysis resources will be focused on assessing high-risk suppliers or components determined from externally provided intelligence or risk reports. When high-risk assessments are identified, they are usually clearly justified based on higher confidence information. This clear justification allows for the risk to be readily communicated between organizations. Due to limited resources in structured procurement and most high-risk information being externally provided, there will be risk uncertainty up to high risks and a default high risk tolerance. A structured procurement does maintain control over the automated process and avoidance responses are possible by removing high risk suppliers or components from the process. The automated procurement aspects also allow for risk transfer to the end user by providing risk notices and the end user must then manage the risk.
- **Engineered** – This procurement generally has engineering resources provided for the custom services to develop the system capability. The procurement contract can be scoped for resources

to be allocated to C-SCRM analysis and even to anticipated risk response efforts. With these resources, internal C-SCRM effort can be applied to not only investigate externally provided high risks, but also to investigate critical component high risk within the system. Through C-SCRM critical component risk analysis, risk assessments will likely identify risks down to moderate levels. These additional C-SCRM resources will lower risk uncertainty to a default risk tolerance of moderate risk.

- **Assured** – This is also a custom engineered procurement but is further customized for complex and high consequence systems that require high assurance. The procurement contract will likely enable fully resourced C-SCRM analysis and risk response effort to be provided. The allocation of significant resources is provided based on the general expectation that risk uncertainty and risk responses will be applied to reduce risk as low as feasible within the acquisition lifecycle. The additional C-SCRM resources should enable thorough risk assessment that identifies risks below moderate risk levels. The risk handling expectations and additional risk assessment effort will set the default tolerance threshold below moderate risk. The risk tolerance should not be low risk based on two primary factors in C-SCRM efforts. Risk assessment is based on intelligence information that provides negative indicators on a component or supplier. If there is a lack of negative indicators, then the risk assessment will likely have lower confidence. Low confidence intelligence can make the overall assessment moot because there is a lack of evidence for risk determination. The other primary factor is related to the risk management responses that require resources to execute. As risk response resources are applied, there is usually a marginal return on mitigation investment to move overall system risk below moderate levels. This marginal return is due to more risks usually existing at moderate levels and therefore more resources are necessary to mitigate the risks and lower the overall system risk. Attempting to assess and manage overall risk down to low levels is not an effective use of resources.

3. Risk Assessment & Mitigations

C-SCRM at the most basic level is a process to manage cyber-based risk from the supply chain. The ability to assess risk from a supply chain threat is primarily separated into two factors: impact and likelihood. The threat likelihood is characterized as a probability determination qualitatively (i.e., judgement) or quantitatively (i.e., calculated) about if the threat will be able to accomplish an attack on a vulnerable component's confidentiality, integrity, or availability. The impact is characterized as the specific damage that will be caused by the component's compromised confidentiality, integrity, or availability.

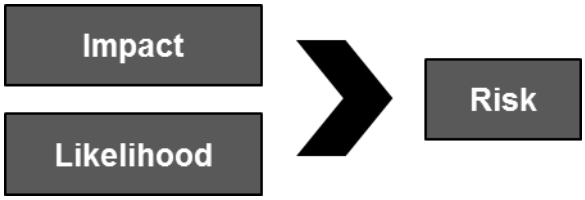


Figure 3 - Main risk components

In seeking to provide a common nomenclature and methodology, this document leverages aspects of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 [4] to frame and describe C-SCRM best practices. Risk assessment as stated in NIST SP 800-30 "is a key component of a holistic, organization-wide risk management process". C-SCRM does not exist in the isolation of cybersecurity responsibilities. C-SCRM risk assessment and management should merge into the overall system security engineering, systems engineering, and organizational risk management practices.

Building upon these basic aspects, C-SCRM risk assessment factors are further defined in the following terms:

- **Mission Impact:** Magnitude of harm resulting from the compromise of a component's confidentiality, integrity, or availability. Impact can be determined through many factors important to the procurement organization, such as operational mission impact, cost, development schedule, loss of life, loss of sensitive information, or reputation.
- **Threat:** A source with intent and method to employ tactics, techniques, and procedures that compromise component confidentiality, integrity, or availability.
- **Vulnerability:** A weakness that can be exploited by the threat.
- **Likelihood:** Probability that a given threat can exploit a vulnerability or predisposing condition.

These factors are utilized in a risk assessment process as depicted in Figure 4. The process is continuously utilized to assess risk as a component's use within a system changes or as new threats and vulnerabilities emerge. This main process is be utilized for each of the procurement type best practices described in the subsequent sections.

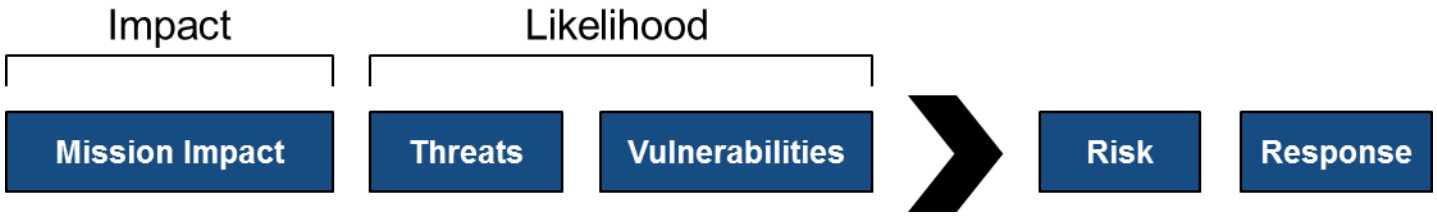


Figure 4 - Basic Risk Assessment Process

3.1 Simplified Procurement Best Practices

As previously described, simplified procurements have little to no additional C-SCRM analysis resources available for making micro-purchases. This situation causes a default high risk tolerance due to an inability to internally investigate supplier risk factors. As shown in Figure 5, the purchaser will not likely be able to specifically address C-SCRM threats in the context of the component use or any vulnerabilities that would exist in the use of the component in a system. In addition, the risk assessment analysis of mission impact caused by the component compromise is not likely known for confidentiality, integrity, or availability.

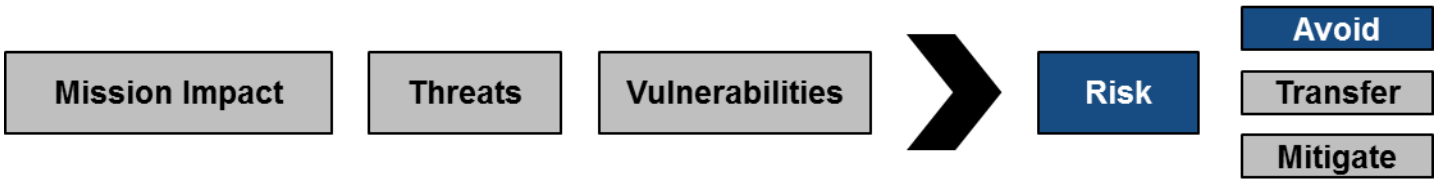


Figure 5 - Simplified Procurement Focus on Externally Provided Risk Assessments

3.1.1 Risk and Response

This situation drives the primary focus to assess risk through existing, external risk assessments. It is incumbent on the purchaser to perform due diligence to investigate external sources for critical risk determinations that have led to suppliers being excluded from DoD purchases through the exercise of appropriate legal authority. The purchaser should seek out this information from their contracting officer, DoD component prohibited supplier lists (e.g., DFARS Subpart 225.7), or from other organizational resources. As an alternative, the purchaser should seek an approved product list if available within the organization. This approved product list will have the due diligence risk assessment already performed on those suppliers to avoid critical or possibly even high risk.

An additional resource to reduce risk uncertainty without requiring significant additional effort is to utilize organization or commercially provided C-SCRM risk assessment services. These services can address C-SCRM factors that give a general picture of risk and through simple ratings a purchaser can readily utilize. These factors can include:

- **Country of Company:** The company resides in a strategic nation state threat that indicates significant risk.
- **Country of Corporate Ownership:** Corporate ownership that resides in a strategic nation state threat that indicates significant risk.
- **Major Financial Obligations:** Major obligations to a foreign nation state that can create liability risk.
- **Cybersecurity Rating:** Risk based off cybersecurity-related risk factors.

A key aspect for utilizing these C-SCRM risk assessment services is to have commodity access to these capabilities. As in no need for individual user licensing to set up and purchase the service. A DoD-wide or DoD component agreement should be obtained to provide such a service that allows all users making a simplified procurement to quickly check for general C-SCRM risk information.

Overall, a simplified procurement's use of externally provided, general risk assessment will only be able to identify critical and some high-risk suppliers. These risk assessments and the limited resources available under the purchase will only allow for the avoidance risk response. The choice to not purchase the component will require the purchaser to seek out a replacement supplier. As a result, the best approach for organization or commercially provided C-SCRM risk assessment services would be to also provide related suppliers as possible substitutions. Otherwise, it will be up to the purchaser to do their own research on a replacement, which will then again need to be vetted through a risk assessment service.

3.2 Structured Procurement Best Practices

Structured procurements are a controlled process that provides access to high-demand, commodity purchased components under standardized contracts. There are resources provided for the set up and management of the structured procurements, which can also include allocations for C-SCRM risk assessment. While there should be some resources available for risk assessment, there will be limits to the risk assessment a structured procurement provider can

perform. The structured procurement provider does not know the specific system use of each component nor the context for the mission the component supports. This limited knowledge will not be able to address mission impact but will be able to assess general threats and vulnerabilities against component types, as shown in Figure 6.

Figure 6 - Structured Procurement Ability to Assess Threat and Vulnerability

3.2.1 Threats and Vulnerabilities

The structured procurement provider should perform due diligence investigations on component suppliers to identify risk within the structured contracts. The "supplier" consideration here is not just the component manufacturer, but also any intermediary vendor that is reselling the manufacturer's component. Threats under investigation should be against strategic or well-known threats that can be clearly identified for critical or high risk. These threat types are primarily focused on foreign ownership, control, or influence (FOCI) situations or specific, higher-confidence intelligence reporting on foreign intelligence entity (FIE) effort to compromise a supplier. A FOCI threat example would be components provided by a Chinese company that is directly or ultimately owned by the Chinese Communist Party. A FIE threat example would be reports of Russian intelligence targeting to compromise a supplier or a specific component.

An additional threat consideration beyond a supplier's FOCI and FIE targeting is where the development of a product occurs. A company may have business attributes (e.g., headquarters, incorporation) for a lower risk country, but may have development (e.g., design, manufacture, sustainment) in a country that has high risk. High-risk countries include Russia because of the System of Operational-Investigatory Measures (SORM) laws. These laws require telecommunications operators to install Federal Security Service hardware that allows the agency to monitor communications metadata and content, including phone calls, internet traffic, and all media. When coupled with other regulations that limit the use of encryption, this FIE access allows for the government to have inside knowledge of all component information developed and communicated across Russian networks, including the Internet. A similar set of national security laws and restrictions on Chinese companies exist for the same FIE access to information and even direct control over companies.

A structured procurement will not likely have enough resources available to perform significant internal threat identification from intelligence. The most likely threat resources available will be organizationally provided threat assessments from the DoD Chief Information Officer (CIO) or DoD Component CIO entities. Requests should be made to these entities for supplier threat information or threat reporting repositories leveraged for information.

Vulnerabilities under investigation should be against suppliers and components that have systemic reporting of vulnerabilities or unmitigated critical vulnerabilities in a component. These situations create a higher likelihood of exploitable vulnerabilities existing in a component or originating from the company itself. For example, this would be a software component with critical vulnerability identified as a Common Vulnerability Enumerations (CVE) in the NIST National Vulnerability Database that has not been patched. This situation would have the component's purchase be immediately exploitable through the vulnerability and would drive critical or high risk. Other vulnerability situations include published reports of previous malicious network intrusions, data breaches, loss of client data, or loss of intellectual property.

3.2.2 Risk and Response

These two aspects of systemic threat and vulnerability against a component, manufacturer, or vendor will enable a basic form of risk assessment to be performed by a structured procurement provider. A structured procurement service provider may also augment the risk assessment by utilizing organization or commercially provided C-SCRM risk assessment services as described under the simplified procurement section 3.1.1. These risk assessment services can also provide detail on the threat or vulnerability aspects associated with the risk ratings.

A fundamental risk response under structured procurement will be to avoid any component with a risk assessment that is critical or clearly high risk. The avoidance response could be in response to a ban through the exercise of appropriate legal authority. However, the avoidance could simply be the structured procurement provider's choice to not list a component, manufacturer, or vendor due to risk judgement. This is not a ban on the supplier, but rather a risk management choice like an approved product list approach to whitelist a supplier within the procurement service.

The alternative risk response is to transfer components with high risk to the end user. This transfer of risk is through a clearly identified risk rating with accompanying threat and vulnerability justification provided. The purchaser will then be able to choose their own risk response of avoidance, by not purchasing the component, or through mitigation if resources are available.

3.3 Engineered and Assured Procurement Best Practices

When a formal procurement has been defined for an engineered or assured solution, there is a fundamental shift in the type of risk assessment and responses possible as engineering resources are made available. This is enabled by the expectation that resources will be provided for C-SCRM risk assessment through system security engineering or cybersecurity budget allocation. As shown in Figure 7, a risk assessment should be able to address all primary aspects of the risk and then perform a risk response of avoidance, transfer, or mitigation. Most importantly, the mission impact portion of the risk assessment with the subsequent criticality analysis will be performed.

Figure 7 - Engineered Procurement Full Risk Assessment and Responses

3.3.1 Mission Impact through Criticality Analysis

With engineering resources available, mission impact can now be fully analyzed for a compromise to confidentiality, integrity, or availability. This mission impact effort is usually called criticality analysis and is utilized to better determine impact under risk assessment. The ability to properly assess risk enables the prioritization of applying limited engineering resources towards the highest risk ratings.

Mission impact should be separated into a definition of the mission and the critical items that support that mission. This primary breakdown of the mission impact under criticality analysis is depicted in Figure 8.

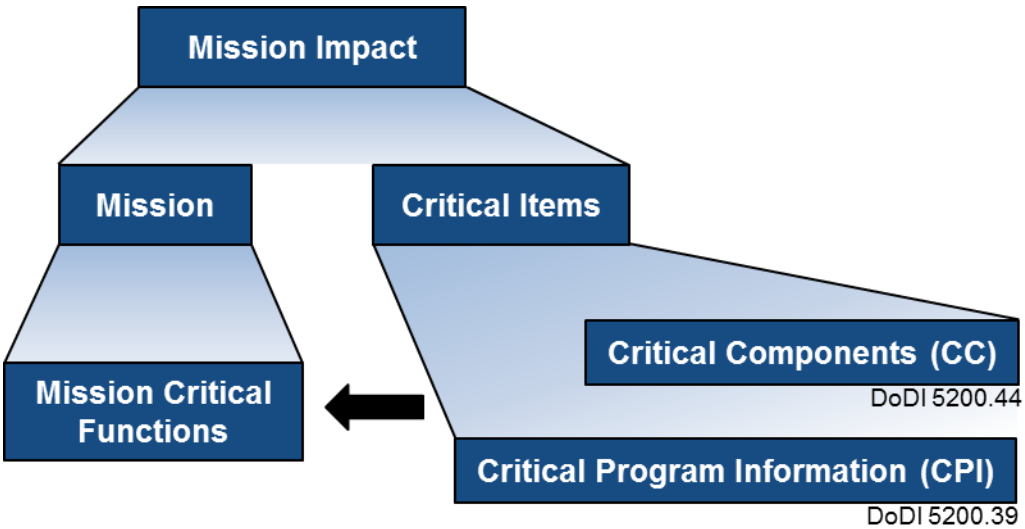


Figure 8 - Decomposition of Mission Impact Through Criticality Analysis

The mission definition can be as simple as a stated purpose for what the procurement will be supporting, all the way up through mission impact aspects defined under the Joint Capabilities Integration and Development System (JCIDS) System Survivability Cyber Survivability Risk Category (CSRC). The CSRC provides distinctions for overall mission type impacts from mission type 1 (MT1) for support systems to MT4 for national or strategic purposes. MT4 is for the most critical defense systems and these procurements will likely fall under assured procurement with the more C-SCRM resources. Engineered procurement will likely only apply for missions up to operational/tactical systems as MT3. See the Cyber Survivability

Endorsement Implementation Guide, Version 1.01 [5] for further details on the CSRC mission types and the analysis process.

No matter how the mission is described, the most important aspect of this process is the definition of critical functions that support the mission. These functions can be derived from program documentation created for the engineered procurement, such as key performance parameters within the initial capabilities document (ICD) or capability description document (CDD), systems specification requirements, concept of operations (CONOPS), or DoD architecture framework (DODAF) views. A list of mission critical functions is utilized as the formal definition of all aspects that need to be protected from a compromise to confidentiality, integrity, or availability.

The matching portion of criticality analysis is the identification of critical items that provide prioritization context for the components being procured. Critical items under C-SCRM analysis are hardware or software critical components (CCs) and components that handle critical program information (CPI). CCs are formally described in DoDI 5200.44 [6] and are primarily information and communication technology (ICT) components that require integrity and availability protection for critical functions. CPI is formally described in DoDI 5200.39 [7] and is basically the information that provides the United States military its technological advantage against adversaries. Components that handle CPI are primarily concerned with protecting the confidentiality of the CPI.

For criticality analysis all components in the system must be identified down to the lowest level possible. This activity is a part of supply chain illumination that involves identifying all components and suppliers within the procurement. The illumination effort must be performed to fullest extent within the government's contractual control, which includes leveraging contractual clauses, information in contractor deliverable content, and direct inquiries to contractors supporting the procurement. For custom engineered components, the component breakdown should not artificially stop at aspects such as a line replaceable unit or subsystem assembly. All logic-bearing components that could be compromised by a threat should be identified. More specifically for software products, a software bill of materials (SBOM) should be acquired from the commercial provider or static analysis tools should be used to perform analysis to generate an SBOM. Software static analysis for composition analysis is used to understand code dependencies and integrated software components. This SBOM analysis can be as complex as hardware component identification.

The identification of CCs can be performed through a top-down or bottom-up process. Top-down CC identification usually occurs during the engineering development process and when design choices are made to procure critical items. If criticality analysis is performed in parallel with the system development, then mission critical functions will be defined, and the supporting CCs will be directly identified when procurement choices are made. Bottom-up identification is usually performed for an existing system that already has all components defined for purchase or components are already deployed within an operational system. This situation usually requires gathering existing lists of components from artifacts (e.g., bill of materials, purchase orders, parts lists) or performing inventory auditing of an operational system. Once the bottom-up list has

been gathered, the components should be mapped to critical functions with a matching impact rating.

CC impact ratings can be to critical functions or more specifically to a component's compromise causing critical loss of confidentiality, integrity, or availability. This mapping of CCs to critical functions is used to create a prioritized list of components that should undergo C-SCRM risk assessment. More specifically, the CC impact mapping can be articulated with gradations of impact (e.g., high, moderate, low) and utilized to prioritize analysis based on risk tolerance. It should be cautioned that a complete gradation ranking process will require effort to perform risk assessment and tracking with subsequent consumption of C-SCRM resources. A procurement should first focus on higher impact components and perform risk assessment on those components, then work down through other components as resources permit. This approach is supported by a moderate risk tolerance that will focus on identifying and mitigating high risks.

The identification of CPI can be an organic effort to determine technological advantage aspects or can be gathered from existing documentation already developed during formal acquisition. Existing documentation that indirectly identifies CPI can be Controlled Unclassified Information (CUI), a program's security classification guide, key performance parameter aspects defined in an ICD or CDD, critical technology lists, or export-controlled information. The identification of CPI can then be matched with components in the system that handle the CPI. CPI may be a CC itself if the CPI is the design information built into the hardware or software. This list of components that handle CPI then need to undergo impact assessment in the manner similar to CCs. Gradations of CPI impact can be set based on criteria such as the example set shown in Table 1. A procurement should focus on components that handle higher impact CPI and first perform risk assessment on those components, then work down through lower impact CPI as resources permit.

Table 1 - Example CPI Impact Criteria

Impact	***Criteria***
High	*- No suitable replacement projected or in development* *- Loss of superiority or movement in relevant battlespace* *- Significant investment level for replacement (funding, time)* *- Technology advantage loss greater than 10 years over adversary*
High-Moderate	*- Replacement fielded in greater than 10 years* *- Loss of battlespace advantage (parity)* *- High investment level for replacement (funding, time)* *- Technology advantage loss greater than 5 years over adversary*
Moderate	*- Replacement fielded in 3-5 years* *- Loss of military advantage; capability replaceable with another system* *- Moderate investment level for replacement (funding, time)* *- Technology advantage loss greater than 3 years over adversary*
Moderate-Low	*- Replacement fielded in less than 3 years* *- Minor investment level for replacement (funding, time)* *- Technology advantage loss less than 3 years over adversary*
Low	*- Loss easily mitigated by changes in CONOPS/tactics* *- Low investment level for replacement (funding, time)* *- Technology easily available*

3.3.2 Threats and Vulnerabilities

With additional C-SCRM resources to investigate threats, a more thorough and tailored analysis is possible for engineered and assured procurements. If available for the engineered procurement a Validated Online Lifecycle Threat (VOLT) or equivalent threat assessment should be referenced for mission specific threats. However, this threat assessment will likely be focused against the mission and may not include supplier specific threat details. Nonetheless, this type of threat assessment will place a basic threat context for the procurement.

More specific to C-SCRM threats, a system security engineer should leverage resources as described for structured procurements. This will include taking the prioritized list of CCs and components that handle CPI and specifically seeking out threat information for higher impact items. For components under analysis that do not have recent or any threat information, additional threat analysis sources should be leveraged to gain further insight. These sources include the Defense Intelligence Agency (DIA) Threat Analysis Center, or the Defense Counterintelligence and Security Agency (DCSA) or similar centers of expertise within a DoD Component, such an office of special investigations or C-SCRM center of excellence. It should be noted that these requests for additional analysis require specific details to be provided about the component to allow the third party to determine specific threats to the component. These details include the specific component (e.g., part or model number), company name, vendor name (if not directly purchased), company location, and context on intended use. If more component details are provided, then a more tailored threat assessment will likely be provided in return.

With respect to vulnerabilities, the additional system security engineering resources will enable investigation into CCs and components that handle CPI vulnerabilities. This analysis includes seeking out published vulnerabilities and some specialized commercial vulnerability sources. Published vulnerabilities include open sources such as NVD CVEs or published reports of compromise as described for structured procurements. Specialized vulnerability sources include commercial services that provide in-depth investigations on companies and products to provide detail beyond openly published content.

3.3.3 Risk and Response

Under an engineered and assured procurement, a complete chain of analysis can be performed for risk assessment. As described in NIST SP 800-30, risk assessment can be initiated with a focus on threat, vulnerability, or impact as the starting point. Based on C-SCRM precedent of criticality analysis, this risk assessment is initiated with an orientation about mission impact determined under criticality analysis. Based on an initial selection of higher impact components and CPI handled by components, threat and vulnerabilities are analyzed to determine the likelihood of the described impact occurring. Likelihood analysis is suggested to incorporate aspects such as threat source characterization (e.g., capability, intent), threat event details for how an exploitation would occur, and linkages to the vulnerability exploitation and existing compensating security controls that would lessen the vulnerability. The calculation of risk can be accomplished in many ways such as a 5x5 matrix of impact versus likelihood ratings.

A high-risk assessment can be directly handled through self-imposed avoidance responses. The procurement can make a design choice to utilize an alternative source if a suitable replacement is available. This approach works best if targeted components are identified early in the procurement design phase, while trades are being made. Avoidance becomes more difficult if the risk is identified late in the procurement and there is little schedule or budget available to replace a component. If the procurement itself is producing a government component to be utilized in a larger system, it is possible to transfer an identified risk to the end system, but this is not advisable. Risk transfer can cause risk aggregation in a large system that can cause systemic and strategic issues that are difficult to mitigate after a component is propagated. Any risk transfer must be closely coordinated with the consumer of the component to ensure they understand the risk being transferred and the consumer can appropriately mitigate the risk.

The additional option available under engineered and assured procurement is direct mitigation of a risk. Mitigation can occur through many design and implementation choices to remove, hide, or actively monitor the risk. One concept advocated is less intrusive means such as: isolation, partitioning, monitoring, virtualization, patch mitigation regimes, hardening, secure configurations, trusted suppliers, parallel operations, assessment and testing, operational practices, and additional cryptographic procedures. The types of mitigation possible are too numerous to list in this document. The mitigation options will be chosen and designed by the engineering support under the procurement. The goal of the mitigation is typically focused on lowering likelihood through lowering the vulnerability aspect or through lowering the impact of the component's compromise.

References

[1] Department of Defense; *DoDI 5000.90 – Cybersecurity for Acquisition Decision Authorities and Program Managers*; December 31, 2020

[2] Draft (2nd) NIST Special Publication 800-161, *Revision 1*; Cybersecurity *Supply Chain Risk Management Practices for Systems and Organizations*; October 2021

[3] Department of Defense; *DoDI 5000.02 - Operation of the Adaptive Acquisition Framework*; January 23, 2020

[4] NIST Special Publication 800-30 Revision 1; *Guide for Conducting Risk Assessments*; September 2012

[5] NIST; *Cybersecurity Framework Version 1.1*; April 2018

[6] Department of Defense; *DoDI 5200.44 - Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*; November 5, 2012

[7] Department of Defense; *DoDI 5200.39 - Critical Program Information Identification and Protection Within Research, Development, Test, and Evaluation*; May 28, 2015

External Distribution

REPORT TITLE
C-SCRM Risk Assessment for Procurement Types

REPORT NO.	PUBLICATION DATE	SECURITY CLASSIFICATION
TOR-2020-02651	September 30, 2020	UNCLASSIFIED

Michele Iversen
DCIO(CS)/RAOI
michele.t.iversen.civ@mail.
mil

APPROVED BY_____ DATE_____
(AF OFFICE)

C-SCRM Risk Assessment for Procurement Types

Cognizant Program Manager Approval:

Jack B. Clarke, PRINCIPAL DIRECTOR
NATIONAL SPACE SYSTEMS ENGINEERING
DEFENSE SYSTEMS OPERATIONS
DEFENSE SYSTEMS GROUP

Technical Peer Review Performed by:

Edgar B. Cruz, SENIOR ENGINEER SPECIALIST
CYBER ENGINEERING DEPARTMENT
CYBERSECURITY AND ADVANCED PLATFORMS
ENGINEERING & TECHNOLOGY GROUP