Assessing DoD System Acquisition Supply Chain Risk Management

By Christopher Alberts, John Haller, Charles Wallen, and Carol Woody

Abstract. Defense capabilities are supported by complex supply chains. This is true for weapons systems and large "systems of systems" that enable force projection — for example, a weapons system like the F-35 Fighter. It is also true for service supply chains — for example, the array of private logistics firms that the Department of Defense (DoD) relies upon to transport personnel and equipment around the world. Important requirements for both capabilities (force projection and transportation) now depend on the cybersecurity and related assurance level of third parties. While supplier, vendor, and contracts relationships provide cost savings and flexibility to the DoD, they also come with risks.

Supply chain cyber risks stem from a variety of dependencies, in particular from the processing, transmittal, and storage of data, and on information and communications technology. These cyber risks in the supply chain are broad and significant. Important mission capabilities can be undermined by an adversary's cyberattack on third parties, even in situations where the government is not explicitly contracting for technology or services like data hosting. In one sense, this risk stems from the reality that virtually all products or services that the DoD acquires are supported by or integrated with information technology.

Software is a critical segment of the defense supply chain. The "Critical Code: Software Producibility for Defense" report states that "software has become essential to all aspects of military system capabilities and operations" [CTSB 2010]. In 1960, software handled just 8 percent of the F-4 Phantom Fighter's functionality. By 1982, it had expanded to 45 percent of the F-16 Fighting Falcon's functionality. By 2000, it handled 80 percent of the F-22 Raptor's functionality [CSTB 2010, p. 19]. In addition, the DoD is increasingly reliant on commercial off the shelf (COTS) products, where the vendor controls knowledge of the details of product functionality. Military systems are not the only ones affected. Software controls virtually everything we use today: cars, planes, banks, hospitals, stores, telephones, appliances, entertainment devices and more.

These supply chain developments pose several unique challenges for the DoD:

- How can leaders ensure that cybersecurity risks in the supply chain are appropriately and optimally identified and mitigated? How can confidence in the supply chain be sustained?
- How can defense organizations measure and improve their ability to manage this type of risk? If an acquisition involves a prime contractor, how can they be sure that the prime contractor is doing so?
- What safeguards need to be in place to recognize and recover from cyber incidents should mitigations prove insufficient? What should happen when mission capabilities are directly affected by changes to supply chains that are out of the government's control?
- How should collaboration, changes and responses be managed nimbly and quickly across supply chains that are normally governed through complex, formal contracts?

Some recent DoD efforts have focused on mandating contractual standards for specific technical controls. For instance, the confidentiality of controlled unclassified defense information shared with contractors has long been a concern. To address this problem, DoD recently modified the Defense Federal Acquisition Regulation Supplement (DFARS) subpart 252.204. Section 252.204-7008 mandates that contractors must institute the controls listed in NIST Special Publication 800-171 to protect "covered defense information" [DFARS 2016]. After much discussion and some consternation in the defense contracting community, DoD subsequently delayed implementation of the revised rule until December 2017. Regardless of the specific timetable, focusing on technical controls in place at the time of contracting is only part of the solution.

A top-down, one-size-fits-all approach to formal acquisition requirements may not account for situations where the appropriate requirements differ from the mandated, specific controls. For example, the controls for private companies that were specified in NIST Special Publication 800-171 were selected for their relevance to the confidentiality of information [Ross 2015]. These controls may not be adequate in situations where the defense capability relies on the availability of systems. In military transportation, for example, this may include the availability of an air traffic control system or a freight forwarding and tracking system.

Defense organizations may be constrained in their choice of contractors. One contractor may be the sole source for a specific, vital capability. Finally, while contractual terms can incentivize and provide guidance to contractors, they hardly form a basis for assurance. In many cases, these controls may only be effective at a single point in time. The government might not be able to tell whether or not a control was actually being maintained.

Cyber risks originating in the supply chain can be made worse by slow internal processes. For example, software-specific issues arise when vendors issue critical security patches for products that reside on classified networks. The lengthy time needed to recertify the software results in delays in applying these patches, leaving systems unnecessarily vulnerable.

Defense organizations need a range of capabilities to manage supply chain cyber risks. These capabilities typically involve additional staff beyond those who are assigned to acquisitions. Leaders should prepare program offices and sustainment depots to address supply chain cyber risks by enhancing their ability to manage supplier performance across a range of capabilities, important practices, and processes.

This article presents a framework of supply chain risk management practices to measure and improve an organization's ability to manage third-party cyber risks. This framework is not a new regulation or policy. Instead, it provides a mechanism for increased confidence about the current level of vendor performance, a fuller understanding of gaps, and a road map for improvement.

Cyber Risks in the Defense Supply Chain: A Growing Challenge

The growing DoD reliance on complex, sometimes global supply chains to deliver military, civil and intelligence capabilities has increased cybersecurity concerns. This complexity makes it more challenging than ever for acquirers to understand, monitor and manage supply chain products and processes.

Managing supply chain cyber risk is especially challenging because that risk is broad and pervasive. The National Institute for Standards and Technology (NIST) defines the Information and Communications Technology (ICT) supply chain as a "linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of ICT products and services and extends through development, sourcing, manufacturing, handling, and delivery of ICT products and services to the acquirer" [Boyens 2012]. However, the related risks often extend to areas which are not explicitly related to information technology, including the following:

- Manufacturing and integration supply chains: Responsible for conceptualizing, designing, building and delivering systems and hardware.
- Service supply chain: Responsible for providing services to acquirers. In a defense context, this includes services that vary as widely as data processing and hosting, logistical services, and support for administrative functions.
- Software supply chain: Responsible for producing the software that runs on vital systems

Each of these supply chains differs in their output, or what they provide to a defense acquirer. As a result, certain vulnerabilities are frequently associated with specific types of supply chains. The software supply chain may introduce vulnerabilities involving open source software modules, such as the Heartbleed security flaw[1]. In addition, there may be risks involving unintended functionality of a particular piece of software. However, DoD faces a similar problem when it comes to each type of supply chain. The security of critical capabilities depends on how well organizations outside direct DoD control address the confidentiality, integrity, and availability of assets that DoD relies upon. Indeed, no particular type of risk is confined to one type of supply chain. DoD must have confidence that effective security and resilience have been built into key systems and services, as well as confidence that they can be sustained. Failures in any of the supply chains that DoD relies on can lead to:

- A breach of confidential information shared with a supplier or vendor.
- A lack of availability of critical service or capability.
- Problems with the integrity of data or systems.
- An attacker maliciously tainting or corrupting the output of the supply chain.

Supply chains are characterized by the need to manage external entities through arm's-length contracts. Unfortunately, the government has a limited ability to verify that good engineering and cybersecurity practices are actually in place. The DoD's ability to properly manage and mitigate these risks should not exclusively rely on either initial contracting processes or the ability to validate controls at the supplier. A framework to help measure, manage and improve DoD capabilities would help to ensure that supply chain risks can be mitigated.

Software: A Case Study in Supply Chain Complexity

To illustrate some of the issues and complexities inherent in managing supply chain cyber risks, we examine the software supply chain as a case study. Software is increasingly taking over functionality previously handled by hardware components. The percentage of system functions performed by software has risen exponentially in recent years. Key benefits include increased flexibility in development schedules and rapid response to changing needs.

However, we are now faced with a situation where the capabilities of today's software technology environment, the need to outsource, and the interaction between off-the-shelf and open source software products have far outpaced our ability to effectively monitor and manage the risk using traditional methods. With the critical roles software holds in our operational environments, the impact of fakes, frauds, and malicious activities could be devastating.

Today's software is riddled with weaknesses and vulnerabilities that represent unacceptable security risks. [McGraw 2006, 3]. The increasingly global nature of software development has also raised concerns that global supply chains could be compromised, allowing malicious code to be inserted into a delivered software product during development or enabling a compromised product to be substituted during delivery or installation.

Like any supply chain, the ownership and responsibility for software may be scattered across several organizations, each of which may affect the security and integrity of the final product. For example, software is often assembled from existing code (see Figure 1 for a hypothetical example). An application may be made up of components from commercial products, open source, and "glue code" that ties these various pre-existing pieces together to provide the desired functionality. Each of these components can also be made up of multiple pieces, and the supply chains can be long with many diverse sources.

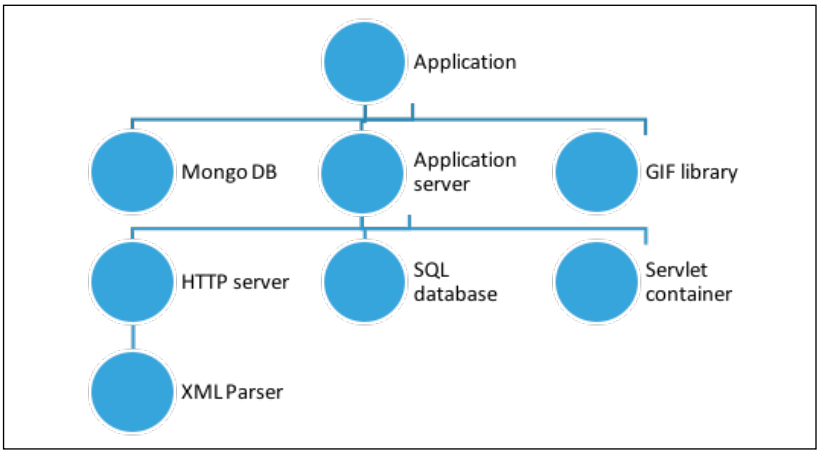

Figure 1

Software Assembled from Existing Code Components

As software is assembled and integrated into a final product, each integrator inherits all of the vulnerabilities inserted by the developers at every sub-level, which can include additional custom, commercial, open source, and legacy software. Software flexibility that allows system users to adjust functionality to meet changing operational needs also provides this same capability to an attacker. In addition, suppliers are often free to update or make changes to the software as needed, which may impact customers (licensees) in unforeseen ways.

The software supply chain comes with an additional complication. Depending on the specific business agreement, an acquirer may have a very limited ability to verify the quality or integrity of the supplied software. A commercial software provider allows use of their product through a licensing arrangement but does not give away the source code. Open source software is frequently also controlled through licensing but with a very different relationship structure: access to the source code is provided and copies of the code can become different products using the original baseline. An organization may also acquire a service which is based on software but the service provider, not the organization, owns the software[2].

The nature of software products has also evolved in recent years with the emergence of computer networks. The focus has shifted from producing stand-alone software products to providing technical capabilities within a larger "system-of-systems" context. A "system-of-systems" is defined as a set or arrangement of interdependent systems that are related or connected (i.e., networked) to provide a given capability. [Levine 2003] This development only increases the number and unpredictability of risks that a government acquirer must take into account.

A common way to control risks in software acquisitions is a formal contract with a supplier. The contract governs the relationship between two organizations and includes a set of requirements. The supplier develops a software product that meets those requirements. Another example of a formal agreement between organizations is when an acquirer licenses commercial off-the-shelf (COTS) software from a supplier. A license outlines any terms and conditions regarding the acquirer's use of the software product.

However, a variety of factors have increasingly made the formal legal contract less effective in terms of mitigating risk in software acquisitions. The complexity of supply chains means that suppliers may have a limited ability to verify that each component of a final product meets the requirement. Software is frequently built for many uses and it can be difficult to determine if it is really "fit for use" in a specific case. Suppliers may be subject to very sophisticated nation-state attacks. Finally, it may be very difficult for the government to prove that a software defect or problem was really the problem in specific cases. This goes directly to a basic question about any contract: How will it be enforced?

Specific technical requirements and contracts: these are the two primary means with which the government has attempted to control cyber risks in the supply chain in the past. While these are basic and foundational methods to control supply chain risk, they increasingly do not suffice. For the government to realize a sufficient level of assurance will require attention to the processes and capabilities employed internally and by key contractors.

Toward Enterprise Management of Supply Chain Cyber Risks: Acquisition Security Framework (ASF)

Commercial, state and federal acquirers have shifted much of the responsibility for addressing supply chain cyber risks in acquisition to integration contractors, software product vendors, and service providers. In many cases, the government will also rely on a prime contractor to sustain systems after the acquisition is complete, taking on the role of directly maintaining the software components and handling this through a service supply chain. This reliance on an intermediary — a prime contractor or integrator — means that the final integrity and suitability of the system depends in large part on how well and maturely the government and prime contractor manage supply chain cyber risks.

The Acquisition Security Framework (ASF) is a way to assess and improve these capabilities. The use cases for the ASF include assessing the capability of relevant organizations to identify and remediate gaps in supply chain risk management capability. While it can be employed as part of due diligence to assess a prime contractor before contract award, its usefulness is not limited to that application. A framework like the ASF could enable groups of contractors to identify and make improvements consistently and collectively for the benefit of an entire acquisition project or community of suppliers. This type of use requires the free and protected exchange of information that concerns not only threats and incidents, but also potentially sensitive information about the practices and internal governance that a contractor has in place.

The ASF was developed from previous work at Carnegie Mellon University's Software Engineering Institute (SEI). In 2014, the SEI's CERT Division developed the External Dependencies Management (EDM) Assessment. It focuses on the capability of critical infrastructure organizations in the United States to manage external dependency and supply chain risks and is an extension of the DHS Cyber Resilience Review (CRR).[3] The EDM Assessment is based on the structure of the CRR and the CERT Resilience Management Model.[4]It provides private sector organizations with a lightweight way to measure their ability to manage this type of risk.

Recently, CERT started investigating how to apply concepts from the CRR and EDM Assessment to help defense organizations evaluate risks and gaps in how they manage supply chains. The initial product is this draft ASF, which is intended to assess supply chain processes for acquiring, engineering and deploying secure software-reliant systems. One application area of particular interest is assessing supply chain processes for DoD weapon system acquisition programs. Focus on such programs will be a priority for this work moving forward.

Risk Factors for Software Supply Chains

Development of the ASF also incorporates an additional, foundational piece of SEI supply chain research. In 2010, an SEI team conducted an applied research project focused on evaluating and mitigating software supply chain security risks across the acquisition life cycle. [Ellison 2010] The 2010 research project led to the identification of the following risk factors for software supply chains in particular:

–Supplier capability: Ensuring that a supplier has good security development and management practices in place throughout the life cycle.
–Product security: Assessing a completed product's vulnerability to security compromises and determining critical risk mitigation requirements.
–Product distribution: Ensuring that the methods for delivering the product to its user are secure and determining how these methods guard against the introduction of malware while in transit.
–Operational product control: Ensuring that configuration and monitoring controls remain active as the product and its use evolve over time.

Framework of the ASF

We designed the ASF to build upon the content and structure of the EDM Assessment to the extent possible. We also designed it to address the four software supply chain risk factors identified in the previous section. The resulting framework comprises five practice areas:

1. Relationship Formation.
2. Relationship Management and Governance.
3. Engineering.
4. Secure Product Operation and Sustainment.
5. Supply Chain Technology Infrastructure.

In the rest of this section, we describe the critical topics to be addressed in each practice area and map them to the supply chain risk areas.

Relationship Formation (Practice Area 1)

Relationship Formation focuses on acquirer practices for evaluating and controlling supplier-related risks before the acquirer enters a relationship with its suppliers. This area also includes practices for contracting with suppliers. Much of the content for this area comes from the corresponding area of the EDM assessment. The following topics are covered in this area of the framework:

–Planning relationship formation.
–Risk management process.
–Supplier capability evaluation.
–Cybersecurity in formal agreements (and in the contracting process).

Relationship Management and Governance (Practice Area 2)

Relationship Management and Governance defines practices for managing ongoing relationships with suppliers. We make heavy use of content from the corresponding area of the EDM assessment when developing practices for relationship management and governance. The following topics are covered in this area of the framework:

–Supplier identification and prioritization.
–Supplier risk management.
–Supplier performance governance and management.
–Change management.
–Supplier transitions.
–Management of supplier access to acquirer assets and technologies.

Engineering (Practice Area 3)

Engineering comprises practices to build appropriate cybersecurity controls into a weapon system and minimize the chance of accidentally inserting vulnerabilities. The following topics are covered in this area of the framework:

–Requirements.
–Architecture.
–Development/coding.
–Integration.
–Testing.
–Independent validation and verification (ensuring product security).
–Deployment (including product distribution).

Secure Product Operation and Sustainment (Practice Area 4)

Secure Product Operation and Sustainment includes practices for managing cybersecurity risk as software-reliant systems are operated and maintained over time. The following topics are covered in this area of the framework:

–Documentation that supports secure product configuration.
–Tools that supports secure product configuration.
–Product updates for security (e.g., software patches).
–Engineering and technical support for managing cybersecurity incidents.

Supply Chain Technology Infrastructure (Practice Area 5)

Supply Chain Technology Infrastructure includes practices for securing technologies that support the execution of supply chain activities. The following topics are covered in this area of the framework:

–Management of acquirer's systems and networks.
–Disruption planning.
–Maintaining and updating control requirements for suppliers.
–Situational awareness requirements for suppliers.
–Procurement of technology (e.g., COTS, open source software, hardware).
–Management of infrastructure dependencies.

	Supplier Capability	Product Security	Product Distribution	Operational Product Control
1. Relationship Formation	x			
2. Relationship Management and Governance	x			
3. Engineering		x	x	
4. Secure Product Operation and Sustainment				x
5. Supply Chain Technology Infrastructure	x	x	x	x

Table 1. Mapping of Practice Areas to Risk Factors

Mapping ASF Practice Areas to Risk Factors

Table 1 shows how the five practice areas of the ASF framework map relate to the four software supply chain risk factors defined earlier in this article. Relationship Formation (Practice Area 1) and Relationship Management and Governance (Practice Area 2) both address supplier capability. Product security and product

distribution are included in Engineering (Practice Area 3). Secure Product Operation and Sustainment (Practice Area 4) provides insight into operational product control. Finally, Supply Chain Technology Infrastructure (Practice Area 5) includes cross-cutting practices that apply to all four risk factors.

The ASF is currently a prototype based on our initial study of software supply chains. It does not represent a conclusive solution to the problem of cyber risks in supply chains. Considerable development and iteration are needed to produce a final baseline version of the ASF framework that includes all relevant cybersecurity practices.

Conclusion

Cyber supply chain risk management has not been broadly and effectively applied across DoD system acquisition and development life cycles. The DoD has already experienced supply chain-related cyber incidents that affected critical systems and capabilities. It also does not appear to have a repeatable, consistent way to measure and mitigate these types of risks across the enterprise. The DoD's efforts to manage this problem have generally involved the inclusion of requirements and specific technical controls in the complex contracts used to govern supply chain relationships. Functional, technical, and security requirements — as well as formal contracts — are certainly elements of supply chain risk management. However, by themselves they cannot provide the speed, flexibility, and repeatability required to manage risks across the entire DoD enterprise and contractor community.

We believe the best predictors of resilience and security across an acquisition are the completeness, efficiency, and institutionalization of the right practices in the relevant organizations. A range of effective practices can be drawn from the management of operational risk in privately owned critical infrastructure. This article identifies a starting point using five operational practice areas that map to high-level risk factors identified in earlier analyses of cyber risks in software supply chains. Further development and use is required to refine this approach. However, through partnership and collaboration, it should be possible to increase the sustainably, effectiveness, and agility with which DoD and industry partners identify, mitigate, and respond to cyber security threats in critical supply chains.

Acknowledgement

Copyright 2016 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Homeland Security or the United States Department of Defense.

REFERENCES

Boyens, J.; Paulsen, C.; Bartol, N.; Shankles, S. A. & Moorthy, R. (October 2012.) "NISTIR 7622: Notional Supply Chain Risk Management Practices for Federal Information Systems." National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.IR.7622

Computer Science and Telecommunications Board (CSTB). (2010.) "Critical Code: Software Producability for Defense." Washington, D.C. (U.S.): National Academies Press. http://www.nap.edu/openbook.php?record_id=12979&page=R1.

Defense Federal Acquisition Regulation Supplement (DFARS) and Procedures, Guidance, and Information (PGI). (May 2016.) "Defense Procurement and Acquisition Policy (DPAP) Website." Section 252.204-7008. http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

Ellison, R. J.; Goodenough, J. B.; Weinstock, C. B. & Woody, C. (2010.) "Evaluating and Mitigating Software Supply Chain Security Risks (CMU/SEI-2010-TN-016)." Software Engineering Institute, Carnegie Mellon University. http://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15176.pdf

Levine, L. Meyers, B. C.; Morris, E.; Place, P. R. H. & Plakosh, D. (February 2003.) "Proceedings of the System of Systems Interoperability Workshop (CMU/SEI-2003-TN-016)." Software Engineering Institute, Carnegie Mellon University. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6469

McGraw, G. (2006.) "Software Security: Building Security In." Upper Saddle River, N.J. (U.S.): Addison-Wesley.

Ross, R.; Viscuso, P.; Guissanie, G.; Dempsey, K. & Riddle, M. (June 2015.) "NIST Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-171

NOTES

1. https://en.wikipedia.org/wiki/Heartbleed
2. For example, at this time, we do not have proven techniques that can find all malicious code that has been inserted into a software component. Part of the difficulty is that in addition to viruses, worms, and Trojan Horses, malicious code can consist of subtle changes that create a vulnerability that an attacker could exploit when the software is deployed. The intent of maliciously inserted code is to change software behavior.
3. https://www.us-cert.gov/ccubedvp/assessments
4. http://www.cert.org/resilience/products-services/cert-rmm/