International Journal of Social Science And Human Research

ISSN(print): 2644-0679, ISSN(online): 2644-0695

Volume 05 Issue 12 December 2022

DOI: 10.47191/ijsshr/v5-i12-69, Impact factor- 5.871

Page No: 5851-5862

Should the Private Sector and Prime Contractors Adhere to the Federal FASC and FedRAMP Regulations?

Donald L. Buresh, Ph.D., Esq.
Touro University Worldwide

ABSTRACT: This article argues that it is in the best interest of private sector organizations and prime contractors to adhere to the Federal Acquisition Supply Chain Security (FASC) and the Federal Risk and Authorization Management Program (FedRAMP) regulations. The paper opines that an organization should follow a supply chain security program, whether from the federal government or otherwise, because such obedience tends to reduce the risk of loss from various factors, including cybercrime. In the modern world, where cyber-attacks from threat actors are common, and the illicit profits gained from such activities can be huge, devotion to a supply chain risk management program is paramount. Thus, loyalty to a supply chain risk mitigation program is critical.

KEYWORDS: Aerojet Case, Federal Acquisition Supply Chain Security Act, Federal Risk and Authorization Management Program, Federal Supply Cain Regulations, Supply Chain Cybersecurity Risk Management

ABBREVIATIONS

The following abbreviations are used in this manuscript:

Abbreviation	Description
Apple	Apple Computer, Inc.
C3PAO	Third-Party Assessment Organizations
CAS	Casualty Actuarial Society
CF	Cybersecurity Framework
CFA	Cyber Fraud Initiative
CIOC	Federal Chief Information Officers Council
CISO	Chief Information Security Officer
CMMC	Cybersecurity Maturity Model Certification
COBIT	Control Objectives for Information and Related Technologies
COSO	Committee of Sponsoring Organizations
C-SCRM	Cybersecurity Supply Chain Risk Management
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
DoD	Department of Defense
DoJ	Department of Justice
ERM	Enterprise Risk Management
FASC	Federal Acquisition Supply Chain Security Act
FCA	False Claims Act
FedRAMP	Federal Risk and Authorization Management Program
HIPAA	Health Insurance Portability and Accountability Act
ISO	International Standards Organization
IT	Information Technology
JAB	Joint Authorization Board
KPI	Key Performance Indicator

NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OUSD A&S	Office of the Under Secretary of the Defense Acquisition & Sustainment
PMO	Program Management Office
RIMS	Risk Management Community, Education, and Resources

INTRODUCTION

This paper attempts to show that it is in the best interest of the private sector and prime contractors to adhere to the Federal Acquisition Supply Chain Security (FASC) and the Federal Risk and Authorization Management Program (FedRAMP) regulations. An organization should follow a supply chain security program, whether from the federal government or otherwise because such obedience tends to reduce the risk of loss from various factors, including cyber-crime. In the modern world, where cyber-attacks from threat actors are common, and the illicit profits gained from such activities can be huge, devotion to a supply chain risk management program is paramount. Thus, loyalty to a supply chain risk mitigation program is critical.

The Federal Acquisition Security Council

The purpose of this section is to present arguments in support of the benefits of centralizing supply chain efforts in an interagency governing body such as FASC. Apple notebooks and mobile devices are used as an example. The relevant FASC factors are listed and shown that they provide a viable framework for federal cybersecurity supply chain risk management if followed. Other options are then considered (e.g., legislation, Executive Orders, etc.), but none compare to a FASC framework. The section concludes that the advantages of FASC appear to override the disadvantages.

FASC Relevant Factors

The FASC is a comprehensive initiative where a single federal organization coordinates various government agencies' supply chain security efforts.[1] The Act was signed into law on December 21, 2018.[2] To appreciate the value of the law, one must understand what the Act covers. A covered article is defined to be:

- Information technology as defined in 40 U.S.C. § 11101;
- Telecommunications equipment defined in 47 U.S.C. § 153;
- The processing of information on a federal or non-federal; information system subject to the requirements Controlled Unclassified Information program or subsequent federal government programs for controlling unclassified information; and
- Hardware, systems, devices, software, or services that possess embedded or incidental informational technology.[3]

In other words, a covered article is essentially any information technology that the federal government employs. A source means any non-federal, supplier, or potential supplier of products or services.[4]

The relevant factors that FASC employs include the functionality and features of the covered article, including its source of data, the user environment where the covered article is installed or used, security, authenticity, and integrity of covered articles and associated supply chains, and he ability of a source to produce and deliver covered articles.[5] Other factors are the ownership of, control of, or influence over covered articles by a foreign government, parties owned or controlled by a foreign government, or other ties between a source and a foreign government, the implications for government missions or assets, national security, homeland security, or critical functions with the employment of the source or covered article, and the potential or existing threats or vulnerabilities of federal systems, programs, or facilities.[6] Still, other factors are comprised of the capacity of the source or the federal government to mitigate risks, the credibility or confidence in available information employed for risk assessment, any transmission of information or data by a covered article to a country outside the United States; and any other information that would factor into a supply chain risk assessment, including any impact to federal agency functions, or any information the FASC deems appropriate.[7]

---

[1] *Federal Acquisition Supply Chain Security Act*, FEDERAL REGISTER (n.d.), *available at* https://www.federalregister.gov/documents/2020/09/01/2020-18939/federal-acquisition-supply-chain-security-act.
[2] *Id.*
[3] 41 U.S.C. § 201-1.101.
[4] *Id.*
[5] 41 U.S.C § 201-1.300(b).
[6] *Id.*
[7] *Id.*

Should the Private Sector and Prime Contractors Adhere to the Federal FASC and FedRAMP Regulations?

Benefits of FASC

The benefits of centralizing supply chain efforts in an interagency governing body such as the FASC stem from the comprehensive nature of the factors used in evaluating sources and covered articles. The scope of coverage demonstrates the value of FASC. For example, consider a notebook from Apple Computer, Inc. (Apple). Apple is a source because it is a non-federal supplier or potential supplier of computing equipment, including mobile devices. A mobile device from Apple or a notebook from Apple is a covered article because:

- It could be construed that it is information as defined by 40 U.S.C. § 11101(6).
- It is likely covered under 47 U.S.C. § 153(52)[8] and (59);[9]
- It could also be subject to the Controlled Unclassified Information program due to its ability to contain and process unclassified information.
- It is hardware that possesses embedded or incidental information technology.

Thus, the relevant FASC factors discussed above apply. An Apple notebook or mobile device is thus subject to a host of controls that would limit its use with the intent of protecting unclassified, confidential, or even classified information.

Other Options

Various other options are available to help the government identify and mitigate supply chain cybersecurity risks, such as legislation, Executive Orders, National Institute of Standards and Technology (NIST) guidance, industry support, and changes to the legal framework. The issue here is that although these possibilities seem adequate on their face, they may suffer from a lack of breadth or specificity. For example, however good as legislation seems, it usually provides a general outline of what the federal government desires to accomplish. Congress typically leaves it up to designated federal agencies to provide specific guidance by making detailed rules for the federal government or private entities to follow. The same observation holds for Executive Orders. The NIST frameworks are voluntary and thus lack the force of law. Industry support may be lacking because businesses are reluctant to share information with the federal government and other businesses without confidentiality or other contractual agreements among the entities that are partaking in the sharing process. Finally, although changing the legal framework seems like a good idea, such efforts are an arduous process that may take a great of time to implement or can be victimized by political machinations. Thus, the other suggested options above are likely not as viable as they appear.

Conclusions Regarding FASC

It appears that FASC is a comprehensive security set of principles that various government agencies could follow. FASC seems to be overall guiding cybersecurity light, providing a framework for different government agencies to use.

Federal Risk and Authorization Management Program

The purpose of this section is to respond to the following questions regarding FedRAMP:

- Does FedRAMP address the same risks and challenges a supply chain cybersecurity assessment program would need to address?
- What complexities exist in the supply chain evaluation that may not be inherent in the FedRAMP evaluation?
- Are there best practices being utilized under FedRAMP that could be applied in the supply chain cybersecurity context?
- Are there ways FedRAMP and a supply chain program could collaborate and work in tandem?

Risks and Challenges

Various federal agencies govern FedRAMP within the Executive Branch. These agencies work collaboratively to develop, manage, and operate FedRAMP. These agencies include:[10]

- Office of Management and Budget (OMB);
- Joint Authorization Board (JAB);
- National Institute of Standards and Technology (NIST);
- Department of Homeland Security (DHS);
- Federal Chief Information Officers Council (CIOC); and
- FedRAMP Program Management Office (PMO).

[8] 47 U.S.C. § 153(52).
[9] 47 U.S.C. § 153(59).
[10] FedRAMP Staff, *Goveranance*, FEDRAMP (n.d.), *available at* https://www.fedramp.gov/governance/,

Should the Private Sector and Prime Contractors Adhere to the Federal FASC and FedRAMP Regulations?

The NIST advises FedRAMP on the Federal Information Security Modernization Act compliance and assists in generating standards for the accreditation of independent certified third-party assessment organizations (C3PAOs).[11] NIST's responsibility is that FedRAMP possesses the security controls that support a supply chain cybersecurity risk assessment program.[12] In particular, NIST ensures that FedRAMP complies with NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations.[13] The security controls for NIST 800-161 are:[14]

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authorization
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Program Management
- Personnel Security
- Provenance
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity

However, the security controls may be different for other supply chain risk management frameworks. A comparison would have to be conducted to ensure that a given supply chain risk management framework was consistent with FedRAMP. Another supply chain risk management framework may be less or even more comprehensive than NIST 800-161. All that can be said is that the FedRAMP framework employs the NIST 800-161 security controls and that FedRAMP and NIST 800-161 address the same risks and have the same challenges.

Complexities in FedRAMP and Supply Chain Evaluations

According to Blanchard, there are the following nine issues in evaluating the issues surrounding a supply chain:[15] First, the design of a global supply chain network should align with customer requirements and expectations. Second, supply chain exception management processes should drive action. Third, sourcing decisions should consider the impact on customer service and profit, not just unit cost or landed cost.[16] Fourth, a single function should be responsible for establishing the value of imported goods and must reconcile financial input from all sources of supply. Fifth, an import classification process should include an audit trail of information. Sixth, corporate-level executives must actively support trade compliance and empower their supply chain executives.[17] Seventh, trade compliance processes must be integrated with supply chain processes. Eighth, unique data that facilitates trade should be accurately created once, stored in a central location, and used repeatedly. Finally, export determination, the appropriate government authorization for your transaction, must be performed on all export shipments.[18]

The complexities associated with a FedRAMP supply chain evaluation and other supply chain evaluations deal with the nine points above. The question asked is whether there are different inherent supply chain complexities in a given framework that are not in the FedRAMP framework. According to Noatum Logistics, in a survey of 124 chief supply chain officers, when asked about their top business pressures, the respondents stated that these pressures included the rising costs of supply chain management (50 percent), the growing complexity of the supply chain (36 percent), and the escalating demand for service from customers.[19] These pressures are likely affiliated with five acute symptoms of supply chain problems over time.[20]

---

[11] Jon Boyens, Celia Paulsen, Hatha Systems, & Nadya Bartol, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) (Apr. 2015), *available at* https://csrc.nist.gov/publications/detail/sp/800-161/archive/2015-04-08.
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] Dave Blanchard, *Nine Tips for Evaluating Your Supply Chain Organization*, INDUSTRY WEEK (Jan. 14, 2007), *available at* https://www.industryweek.com/supply-chain/article/22011327/nine-tips-for-evaluating-your-supply-chain-organization.
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Supply Chain Network Evaluation: Assessing the Health of Your Supply Chain*, NOATUM LOGISTICS (2012), *available at* https://www.miq.com/resources/white-papers/supply-chain-network-eval-white-paper/.
[20] *Id.*

The following issues are red flags that demand a close examination of cybersecurity and logistics management practices:[21]

- When something is new, current practices and processes will likely not be effective in the future;
- When transportation costs are rising, a review of the supplier base may be necessary to become more competitive;
- When shifting a source, there may be a significant impact on a supply chain;
- When entities are divested or acquired, logistic strategies that used to work may no longer be effective; and
- When infrastructure costs are rising, a modification in the number and location of distribution centers may be necessary.

Generally, a supply chain evaluation addresses inventory positioning, distribution facility footprint, and the transportation that links facilities, suppliers, and customers.[22] At a more detailed level, a supply chain evaluation should identify opportunities to reduce overall shipping costs by combining shipments to meet current business needs, find opportunities to lower transportation costs, and improve service by shifting modes based on supplier density, shipping frequency, and shipment characteristics, and lower transportation costs and improve service by evaluating the current carrier mix, rate structures, service metrics, and asset availability.[23] A supply chain evaluation should also evaluate whether suppliers a filling purchase orders on time and without unnecessary shipments, analyze electronic and manual invoice processing systems to ensure that invoices are rated correctly, and review ways to reduce carbon emissions while benefiting from federal and state financial incentives.[24] Finally, a supply chain evaluation should think about relocating or closing facilities to maximize profits and consider reducing the number of employees or reallocating current employees via technology.[25] Different supply chain evaluations may address some or all of the abovementioned issues. Any gaps are likely possible when comparing a FedRAMP evaluation with other supply chain methodologies.

Best Practices

As previously stated, FedRAMP employs the NIST 800-161 supply chain risk management framework. According to Marker, the best supply chain risk management frameworks are:[26]

- The Casualty Actuarial Society (CAS) Enterprise Risk Management (ERM) Framework;
- The Committee of Sponsoring Organizations (COSO) ERM Integrated Framework;
- The International Standards Organization (ISO) 31000 ERM Framework;
- The Control Objectives for Information and Related Technologies (COBIT) ERM Framework;
- The NIST ERM Framework; and
- The RIMS Risk Maturity Model ERM Framework.

The question is which one of these frameworks contains the best practices. This query is difficult to answer without analyzing each framework in detail. What can be said is that the three most likely candidates are the ISO 31000 framework, the NIST framework, and the RIMS risk maturity model framework. These frameworks may be equivalent. Isomorphic mappings should exist from one framework to the other. If so, then one framework is as good as another. Hopefully, this is the case.

Collaboration

Could or should a FedRAMP supply chain program collaborate with another supply chain program? If the helping verb is "could," the answer is obviously yes. However, if the helping verb is "should," a completely different response is appropriate. Suppose one supply chain program is a best practice while the other has deficiencies. In that case, an entity should gravitate towards a better supply chain program and abandon the inferior supply chain program. Why accept less than the best? There is no reasonable justification for doing so. Thus, the answer to the collaboration question is to adopt the best supply chain program and abandon the other one. It just makes sense.

Conclusions Regarding FedRAMP

This section addressed the risks and challenges of a cybersecurity supply chain program and the complexities of a FedRAMP evaluation. The section discussed best practices in a cybersecurity supply chain context. Finally, the piece noted the issues when FedRAMP collaborated with another supply chain program. The analysis above observed that FedRAMP likely employed a NIIST 800-161 supply chain risk management framework. This means that any analysis of FedRAMP is likely equivalent to an analysis of NIST 800-161. The

[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] Andy Marker, *Enterprise Risk Management Frameworks and Models*, SMART SHEET (Nov. 2, 2021) *available at* https://www.smartsheet.com/content/enterprise-risk-management-framework-model.

reason is that NIST advises FedRAMP on the Federal Information Security Modernization Act compliance and assists in generating standards for C3PAOs. NIST ensures that FedRAMP possesses the security controls that support a supply chain cybersecurity risk assessment program.

Private Sector and Federal Regulations

This section discusses whether private sector businesses that do business with the federal government would be subject to federally imposed cybersecurity risk management security requirements are realistic or likely to succeed. The answer to this question is heavily dependent on what the government requires cybersecurity risk management framework. Some cybersecurity risk management frameworks may be more or less restrictive than others. The more restrictive the framework, the more likely fewer companies will be willing to do business with the federal government. The reason is probably that the more restrictive a framework is, the more expensive the framework is to implement. Small companies do not have the revenue to implement a restrictive security framework.

On the other hand, with a flexible security framework, many companies can employ it. Small companies can apply a flexible security framework because of the fluidity of the

framework. In other words, a flexible risk management framework is likely to provide more opportunities for small companies, thereby giving the federal government a large vendor base. Thus, there is a balance between the rigidity or restrictiveness of a risk management framework and the number of potential vendors when deciding whether a cybersecurity supply chain risk management framework is realistic or likely to succeed.

FASC Supply Chain Standard

Suppose that the FASC framework is the presumed security framework selected by the government. The reason is that the framework is well known among federal agencies and because it seems to have the appropriate balance between flexibility and rigidity. It is a comprehensive initiative where a single federal organization coordinates various government agencies' supply chain security efforts.[27] However, for various reasons, some small companies may not be able to implement an extended version of FASC. Suppose a small company chooses to implement a flexible version of FASC. In that case, there is a distinct possibility that the federal government may not approve of its implementation, thereby leaving the firm with high costs and no benefits.

Is FASC a Realistic Standard?

FASC seems to be a realistic standard that entities can employ successfully for mid-range to large companies. However, FASC may be an unrealistic framework for small companies because the company is too small to expend its resources on implementing the standard. What is the firm's size that determines whether it can adhere to the standard? Size can be measured in various ways, where annual revenue and the number of employees are two different measures. Entities with substantial revenue can hire independent contractors that may assure FASC compliance. However, when the number of employees measures the corporate size, a firm may not be able to have the appropriate staff or the financial resources to ensure complete FASC compliance. Small companies' staff is typically dedicated to generating revenue, not assuring compliance with a federal government standard. From a size perspective, firms can be divided into the following three categories:

- Companies that can quickly implement the FASC standard;
- Firms that may have financial or process difficulties in implementing the FASC standard; and
- Entities that are too small to implement the FASC standard.

There is nothing to discuss for an organization in the first category. If they decide to contract with the federal government, a FASC implementation is merely the cost of doing business. The firm may decide that implementing FASC is a viable growth path for an organization in the second category. On the other hand, the corporation may decide that it wants to grow in other areas or finds that a FASC implementation is too expensive or high risk. Each firm is different depending on the business and financial circumstances in which it finds itself.

Entities that are too small to implement the FASC standard are organizations that have existed for many years or are startups. The firms that have existed for years probably decided to remain small because the founders did not want to grow the organization beyond a size usually only known to themselves. As for startups, they may or may not possess venture capital and are likely dedicated to developing a marketable product. A startup may want to implement the FASC standard in the future when it has more revenue and employees. This desire may only be known to the founders or select senior management. A small organization can be characterized as having 25 or fewer employees.

[27] *Federal Acquisition Supply Chain Security Act*, FEDERAL REGISTER (n.d.), *available at* https://www.federalregister.gov/documents/2020/09/01/2020-18939/federal-acquisition-supply-chain-security-act.

Should the Private Sector and Prime Contractors Adhere to the Federal FASC and FedRAMP Regulations?

Outcomes If Firms Do Not Comply

There are several possible outcomes if a FASC-compliant firm becomes non-compliant. First, the company can end its relationship with the federal government. Second, the federal government can cite the company for non-compliance and give the organization time to return to compliance. Finally, the federal government can terminate its relationship with the firm because of non-compliance.

Conclusion Regarding the Private Sector and FASC Regulations

The success of a cybersecurity supply chain framework, such as FASC, depends on the organization's size implementing it and the desire of the entity to do business with the federal government. If, for a moment, ignore the business proclivities of a firm, what is left is its size, either in revenue or number of employees. Based on the conversation above, the number of employees is critical when deciding whether a cybersecurity supply chain framework will be realistic or successful. The bigger the company, the higher the likelihood of success. Even so, small companies may have difficulties implementing a supply chain framework. Mostly, small organizations are more focused on being solvent than adhering to a specific cybersecurity supply chain framework. This author believes that firms with 25 or fewer employees will likely not implement such a framework as FASC because they may not see it as a revenue-generating vehicle. However, this opinion may change as a company grows, depending on its inclination to become a government contractor.

Prime Contractors and Federal Regulations

In the Book of Genesis, Cain and Able were the first two sons of Adam and Eve. Cain, the oldest child, was a farmer, whereas Able, the younger child, was a shepherd. Both made sacrifices to God, but God accepted Able's offering but not Cain's. When Cain and Able went into the field, Cain killed Able. Later, God appeared to Cain and asked him where Able was. Cain replied, "I do not know: am I my brother's keeper?"[28]

Cain's response to God forms the basis of whether prime contractors should be responsible or liable for the cybersecurity efforts of their sub-contractors. If not, legal liability ends with the prime contractors but does not extend to the subcontractor. This is an unsatisfactory answer because cyber-attacks can originate from a sub-contractor, and it seems reasonable for sub-contractors to be subject to verification by a prime contractor. On the other hand, if it is appropriate for prime contractors to be responsible or liable for the cybersecurity efforts of their sub-contractors, the obvious question is when the prime contractor's liability ends. The situation is similar to the relationship between actual causation (but-for causation) and proximate causation (foreseeable causation) in tort. If proximate causation is ignored, actual causation can extend well outside the range of reasonableness. Actual causation is capable of extending infinitely backward in time. However, in its wisdom, the legal profession has seen fit to limit actual causation by appropriately applying reasonable foreseeability or proximate causation to cut off a causal chain.

There can be layer upon layer of sub-contractors in today's world of just-in-time inventory and supply chain management. The layers can extend three, four, or more layers deep. The issue facing a prime contractor is how many layers deep should a prime contractor traverse to ensure that a supply chain is secure. The deeper the prime contractor goes down the rabbit hole, the more expensive it becomes to monitor the security systems of its sub-contractors. It can become economically and financially prohibitive to monitor the security efforts of sub-contractors that are too removed or distant to manage. On the other hand, creative cybercriminals are likely to search for far-removed sub-contractors to infect their systems with malware with the hope that the offending code will somehow make its way into the prime contractor's systems.

This is the dilemma facing prime contractors. A prime contractor can dramatically increase its costs and evaluate the security systems of every single sub-contractor regardless of its relationship with the prime contractor, or a prime contractor can limit its examination of its sub-contractors to a pre-specified communication level below the prime contractor and assume the risk that a breach may occur at the level of a distant sub-contractor. There is no royal road here. It is just a matter of what is an acceptable risk and at what cost.

Benefits of Making Prime Contractors Responsible

According to the Department of Justice (DoJ), for companies doing business with the federal government, the benefits of making prime contractors responsible for the security efforts of their sub-contractors include:

- "Building overall resiliency against cybersecurity intrusions across the government, the public sector, and key industry partners.
- Holding contractors and grantees to their commitments to protect government information and infrastructure.
- Supporting government experts' efforts to timely identify, create and publicize patches for vulnerabilities in commonly-used information technology products and services.

[28] Genesis 4:1-9.

- Ensuring that companies that follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage.
- Reimbursing the government and the taxpayers for the losses incurred when companies fail to satisfy their cybersecurity obligations.
- Improving overall cybersecurity practices that will benefit the government, private users and the American public."[29]

Costs of Making Prime Contractors Responsible

The problem with the announcement from Deputy Attorney General Lisa O. Monaco is that there are no costs or disadvantages listed in the press release. There is no such thing as a free lunch. There is no such thing as a product or service with benefits without costs and advantages without disadvantages. The hidden assumption of the announcement is that the benefits overshadow the costs. This assumption may not be correct. It could turn out that costs surpass benefits. It is necessary to bring forth the costs, or at least those issues that contribute to cost so that the hidden assumption can be examined in the light of reason.

Cybersecurity Maturity Model Certification

Although the Cybersecurity Maturity Model Certification (CMMC) is not yet set in stone, the cost of compliance for the Cyber Fraud Initiative (CFI) or the CMMC has yet to be determined. It should be remembered that the Department of Defense (DoD) is driving the CMMC into existence. The CMMC standard will likely affect 300,000 businesses in the DoD supply chain.[30] The CMMC has recently been revamped, where there are now three levels instead of five. The levels are:[31]

- Level 1 – This is the foundational level that requires 15 controls that come from FAR 52.204.21, an essential federal government rule safeguards covered contractor information systems.[32]
- Level 2 – This is the advanced level based on Level 3 of the old CMMC model. Under this level, a contractor is subject to an independent third-party assessment every three years from a C3PAO.[33]
- Level 3 – This is the expert" level. It replaces Levels 4 and 5 of the previous model and includes 110 controls mandated by Level 2 and compliance with NIST SP 800-172.[34]

Some factors that contribute to the cost of compliance are the level of CMMC required to be determined, the amount of controlled unclassified information (CUI) the company handles, and the Information Technology (IT) support resources available such as training and overall capacity.[35] Other factors include The size and complexity of the network depending on the size of the entity, the age of the equipment where older equipment is usually more costly to secure, the number of facilities, and the use of cloud-based applications.[36] According to Katie Arrington, the Chief Information Security Officer (CISO) of the Office of the Under Secretary of the Defense Acquisition & Sustainment (OUSD A&S), the assessment for Level 1 probably costs between $3,000 and $5,000, with costs increasing as an entity moves from Level 1 to the higher levels.[37]

The Aerojet Case and Its Consequences

On April 27, 2022, the jury was immediately impaneled, but before the trial began, Aerojet agreed to pay $9 million to settle the case.[38] The case was brought under the False Claims Act (FCA) by Aerojet's former senior director of cybersecurity, to the Eastern District of California, on behalf of the government.[39] The whistleblower alleged that Aerojet had lied to the government regarding its cybersecurity

---

[29] DoJ Staff, *Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative*, DEPARTMENT OF JUSTICE: OFFICE OF PUBLIC AFFAIRS (Oct. 6, 2021), *available at* https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

[30] Sea Glass Technology, *How Much Does A CMMC Certification Cost?*, SEA GLASS TECHNOLOGY (Apr. 4, 2022), *available at* https://www.seaglasstechnology.com/how-much-does-a-cmmc-certification-cost/.

[31] Id.

[32] *FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems*, ACQUISITION.GOV (May 26, 2022) *available at* https://www.acquisition.gov/far/52.204-21.

[33] Sea Glass Technology, *supra*, note 3.

[34] *Id.*

[35]

[36]

[37] *Id.*

[38] B. Stephanie Siegmann, *The Future of DOJ's Civil Cyber-Fraud Initiative After Aerojet*, HINCKLEY ALLEN (May 19, 2022), *available at* https://www.hinckleyallen.com/publications/the-future-of-dojs-civil-cyber-fraud-initiative-after-aerojet/.

[39] *Id.*

compliance to get contracts with DoD and NASA from 2013 to 2015. The whistleblower petitioned the court for damages above $19 billion, or three times the amount of every invoice that was paid under the fraudulent contracts.[40]

It is not surprising that the DoD will likely aggressively pursue cyber-related claims under the FCA.[41] Siegmann recommended that contractors and sub-contractors become NIST SP 800-171 compliant to avoid DoD litigation. Given that CMMC is not expected to be publicly available until March 2023, there is not a lot of time for firms to become CMMC compliant.[42] If the DoD intends to sue its contractors for cyber-related violations, the potential penalties could force a contractor or sub-contractor into Chapter 7 or at least Chapter 11 bankruptcy. *Aerojet* is a case in point, where had the case gone to trial, the damages could have permanently left the firm in financial ruin. This situation might not have benefited the DoD, mainly if Aerojet produced mission-critical products or services.

Thus, there are two costs that should be considered: the cost of compliance and the cost of non-compliance, where the non-compliance could be negligent rather than intentional.

How to Improve Visibility in a Supply Chain

According to Javaid, the five ways to improve the visibility in a supply chain include

- Analyzing the supply chain.
- Identifying pain points and prioritizing based on strategic goals and objectives.
- Improving collaboration with suppliers, partners, and competitors.
- Balancing digital technology and dexterity; and
- Measuring and improving with the help of key performance indicators (KPIs).[43]

Analyzing a supply chain is critical because it helps identify points of pain. Once the pain points are identified, they need to be prioritized to address the more painful points first. Third, an entity should collaborate with its suppliers, partners, and possibly competitors to minimize the consequences of its critical pain points without violating antitrust law by cooperating with its competitors. Next, balancing digital technology with dexterity is essential, mainly due to the covid pandemic. Finally, KPIs should be expressly defined so that supply chain visibility can be noticeably improved.[44]

Conclusions Regarding Prime Contractors

Although supply chain security is essential in this cyber age, care should be taken so that what is implemented is firm but flexible. Security should not force an excessive number of small companies out of business. It should allow the government to satisfy its needs without unnecessary delays caused by the lack of a critical contractor or sub-contractor. This is no mean feat, but it is something that should be remembered. Lack of flexibility and diversity is not a strength but a weakness.

Private Sector versus the Public Sector Approaches

This section aims to compare the public sector approach to supply chain cybersecurity risk management to the private sector approach. The section argues that the public sector approach is superior to the private sector approach for the reasons stated herein. This argument does not deny the value of the private sector approach. Instead, it only points out that the public sector approach has more value than the private sector approach and that organizations should look to the public sector as a guide in implementing a supply chain cybersecurity risk management framework.

Supply Chain Cybersecurity Risk Management

Supply chain cybersecurity risk management is an issue common to organizations in the public and private sectors. According to NIST, cybersecurity supply chain risk management (C-SCRM) is "the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/OT product and service supply chains."[45] C-SCRM encompasses a system's life cycle, including design, development, distribution, deployment, acquisition, maintenance, and destruction.[46] It should be remembered

[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] Shehmir AJavaid, *5 Steps to Improve Supply Chain Visibility in 2022*, AI MULTIPLE (Mar. 14, 2022), *available at* https://research.aimultiple.com/supply-chain-visibility/.
[44] *Id.*
[45] NIST Staff, *Cyber Supply Chain Risk Management (C-SCRM)*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Feb. 7, 2017), *available a*t https://csrc.nist.rip/scrm/.
[46] *Id.*

that supply chain threats and vulnerabilities can compromise a system, product, or service at any stage and may do so intentionally or unintentionally.[47]

In protecting a supply chain from cyber threats, a variety of frameworks are available, including NIST 800-53, the Cybersecurity Framework (CF), the Cybersecurity Maturity Model Certification (CMMC), and a host of other industry-specific frameworks (e.g., the Health Insurance Portability and Accountability Act (HIPAA) framework).

Comparison Between the Two Approaches

When comparing the approach by the public sector versus the private sector regarding C-SCRM, it is evident that the framework selected may not be the determining characteristic since both public and private entities can select the same framework. The critical differences lie in how a particular framework is implemented. The following table lists the differences between the public and private approaches:

Public Sector Approach	Private Sector Approach
C-SCRM frameworks are mandatory.	C-SCRM frameworks are voluntary.
Implementation of a C-SCRM framework is extensive and rigid.	Implementation of a C-SCRM framework is flexible.
Specific C-SCRM frameworks are required by federal law or executive order.	Specific industries, such as the finance or health industries, are required to employ a C-SCRM framework by the federal government or federal law. Other industries that are not subject to federal law or regulation are under no such obligation.
Federal agencies are required to follow federal law or executive orders.	Companies not affiliated with the federal government possess a great deal of latitude.
Federal agencies must extensively monitor the security efforts of all their suppliers	Companies may monitor the security efforts of their suppliers but may not monitor all of their suppliers.
Except for classified information, data are generally accessible because of the existence of transparency laws.	Companies generally hold data secret and are not accessible.

Why the Public Sector Approach May Be Better

The public sector approach is better than the private one for the reasons listed in the table above. The risk management framework is mandatory, meaning that all federal agencies must implement a cybersecurity supply chain risk management framework. There are no exceptions. This assures individuals and other federal agencies that the data stored by a compliant entity is secure. The risk management frameworks advocated by the federal government are extensive and rigid, meaning that a third party clearly understands how data are being protected. Third, there are specific C-SCRMs that a federal agency must implement. For example, the DoD mandates that any of its agencies, contractors, and sub-contractors implement CMMC. Because CMMC is detailed and extensive, this fact further assures a person that data are secure.

A federal agency must follow federal law and executive orders. In terms of C-SCRM, this fact implies that a person can be assured that the federal agency is implementing the C-SCRM according to rigorous specifications. Next, according to the Civil Cyber-Fraud Initiative, federal agencies must monitor themselves and the C-SCRMs of their contractors and sub-contractors. Again, this fact gives further confidence that data are protected. Finally, except for classified data and CUI, data are publicly accessible in the public sector. This fact allows an individual to verify that data are protected. Thus, the public sector approach to supply chain cybersecurity risk management is better than the private one for the above reasons.

Benefits to Be Gained from Both Sectors Working Together

The benefit of the public and private sectors working together is one receives the best of all possible worlds. In other words, the synergies that appear when both approaches work in harmony exceed the sum of their parts. When both approaches work in unison, the result is a situation where the advantages of both approaches mesh, forming a greater whole. It is a reasonable thing to do.

[47] *Id.*

Conclusions Regarding the Comparison

This section argued that the public sector approach to supply chain cybersecurity risk management is better than the private sector approach. That said, it does not mean the private sector approach is without value. All that has been shown is that when the two approaches are compared, the public sector approach is more effective than the private sector approach. It is as simple as that.

CONCLUSION

This paper asked whether the private sector and prime contractors should adhere to the federal FASC and FedRAMP regulations. The paper argued that following these standards would be in an organization's best interest. Although there are disadvantages to the FASC and FedRAMP regulations, the article concluded that the advantages outweigh the disadvantages. The issue is that the supply chain risk of disclosing confidential information is significant, warranting the employment of federal or otherwise standards to mitigate the risk. With the advent of the Internet and the storage of corporate data on the cloud, gone are the days when an entity could rely on its resources to protect confidential information. With more advanced technology comes more significant and different risks of loss. Corporations are well-advised to address these risks vigorously so that the risk of loss is mitigated and minimized.

REFERENCES

1) Federal Acquisition Supply Chain Security Act, FEDERAL REGISTER (n.d.), available at https://www.federalregister.gov/documents/2020/09/01/2020-18939/federal-acquisition-supply-chain-security-act.
2) 41 U.S.C. § 201-1.101.
3) 41 U.S.C § 201-1.300(b).
4) 47 U.S.C. § 153(52).
5) 47 U.S.C. § 153(59).
6) FedRAMP Staff, Goveranance, FEDRAMP (n.d.), available at https://www.fedramp.gov/governance/,
7) Jon Boyens, Celia Paulsen, Hatha Systems, & Nadya Bartol, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) (Apr. 2015), available at https://csrc.nist.gov/publications/detail/sp/800-161/archive/2015-04-08.
8) Dave Blanchard, Nine Tips for Evaluating Your Supply Chain Organization, INDUSTRY WEEK (Jan. 14, 2007), available at https://www.industryweek.com/supply-chain/article/22011327/nine-tips-for-evaluating-your-supply-chain-organization.
9) Supply Chain Network Evaluation: Assessing the Health of Your Supply Chain, NOATUM LOGISTICS (2012), available at https://www.miq.com/resources/white-papers/supply-chain-network-eval-white-paper/.
10) Andy Marker, Enterprise Risk Management Frameworks and Models, SMART SHEET (Nov. 2, 2021) available at https://www.smartsheet.com/content/enterprise-risk-management-framework-model.
11) Federal Acquisition Supply Chain Security Act, FEDERAL REGISTER (n.d.), available at https://www.federalregister.gov/documents/2020/09/01/2020-18939/federal-acquisition-supply-chain-security-act.
12) Genesis 4:1-9.
13) DoJ Staff, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative, DEPARTMENT OF JUSTICE: OFFICE OF PUBLIC AFFAIRS (Oct. 6, 2021), available at https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.
14) Sea Glass Technology, How Much Does A CMMC Certification Cost?, SEA GLASS TECHNOLOGY (Apr. 4, 2022), available at https://www.seaglasstechnology.com/how-much-does-a-cmmc-certification-cost/.
15) FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems, ACQUISITION.GOV (May 26, 2022) available at https://www.acquisition.gov/far/52.204-21.
16) Sea Glass Technology, supra, note 3.
17) B. Stephanie Siegmann, The Future of DOJ's Civil Cyber-Fraud Initiative After Aerojet, HINCKLEY ALLEN (May 19, 2022), available at https://www.hinckleyallen.com/publications/the-future-of-dojs-civil-cyber-fraud-initiative-after-aerojet/.
18) Shehmir AJavaid, 5 Steps to Improve Supply Chain Visibility in 2022, AI MULTIPLE (Mar. 14, 2022), available at https://research.aimultiple.com/supply-chain-visibility/.
19) NIST Staff, Cyber Supply Chain Risk Management (C-SCRM), NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Feb. 7, 2017), available at https://csrc.nist.rip/scrm/.

MISCELLANEOUS CONSIDERATIONS

Author Contributions: The author has read and agreed to the published version of the manuscript.
Funding: This research received no external funding.
Institutional Review Board Statement: Not applicable.
Informed Consent Statement: Not applicable.
Conflicts of Interest: The author declares no conflict of interest.
Acknowledgments: I acknowledge the insights on supply chain cybersecurity risk management that I received from Prof. Amy Apostol.