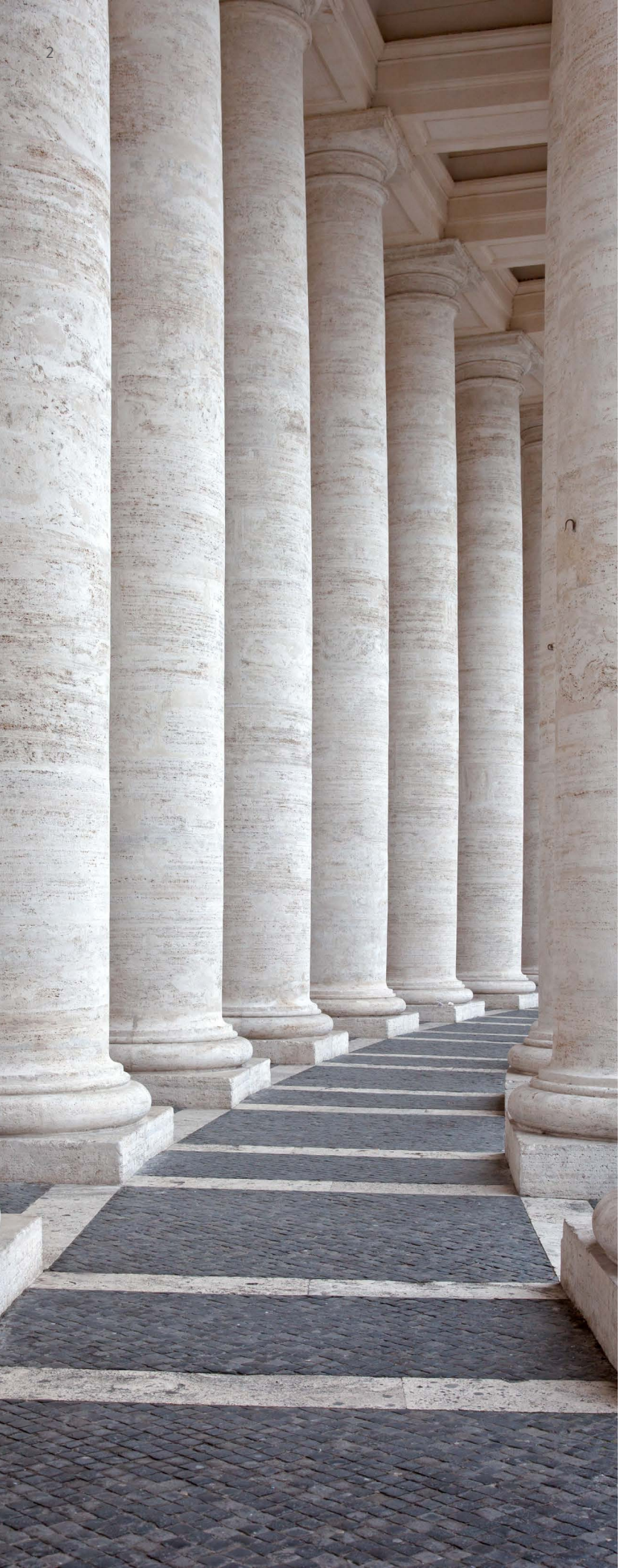
ADG Insights

Supply chain: Emerging issues for ADG companies in the U.S. government market

Supply Chain Series, Volume 2
December 2018

Hogan Lovells



Intro

At a June 2018 House Armed Services Committee (HASC) hearing, the Department of Defense (DoD) announced its "Deliver Uncompromised" initiative, which aims to "establish security as a fourth pillar in acquisition, on par with cost, schedule, and performance, and to create incentives for industry to embrace security, not as a 'cost center,' but as a key differentiator." As we noted in an earlier publication, there is now a need for a robust dialogue between the U.S. government and the aerospace, defense, and government services (ADG) contractor community about how to effectively address supply chain security risk without over-burdening contractors (and, in turn, taxpayers). The challenge of ensuring supply chain integrity is great, and failing to meet this challenge could result in debilitating damage to our national security. At the same time, an enhanced supply chain integrity program must be carefully tailored to avoid impairing the ability of the DoD and government contractors to utilize the best and most efficient manufacturers and creators, no matter where located.

In this piece, we aim to further the important dialogue between contractors and the DoD relating to supply chain integrity. Whatever the ultimate outcome of this dialogue, it's clear that ADG contractors have an opportunity to gain a competitive advantage by bolstering their existing programs to ensure supply chain integrity, or possibly just readying their existing programs for examination and review by the DoD. Contractors who can demonstrate to the DoD that they have a robust supply chain integrity program in place could differentiate themselves from competitors.

The challenge ahead

It is a critically important goal to elevate security considerations in the acquisition process and to offer a genuine incentive for companies to compete to provide a demonstrably secure product or service. Whether elevating security to be a fourth pillar will provide adequate incentive is open to question,[1] but establishing security as a separate pillar is an excellent way to get everyone's attention, including government procurement officials, ADG prime contractors, and the underlying supply chain.

There are, however, many questions raised by the prospect of elevating security to a fourth pillar or otherwise requiring supply chain integrity. How would it work? Can it be achieved in a manner that does not so burden the acquisition process that it impairs the government's ability to obtain good value, or worse, impairs the government's ability to stay a step ahead of our adversaries and competitors? Would requirements be imposed with respect to existing contracts, and if so, who would bear the costs of those new requirements? Would the costs of meeting new requirements undercut the willingness of contractors to identify security issues? Would contractors fear that they would injure their prospects for new business if they discover and disclose security flaws in old or new products?

Before diving into these questions, we need to be clear on what we mean by the supply chain. Most of the discussion seems focused on a particular element of the supply chain – software. This focus is understandable for two reasons. First, software is embedded in articles in a manner that is difficult to see. Second, software provides a potential link between the article and the internet, and therefore has the potential to provide what could be highly sensitive information to a hostile actor or to receive instructions from a hostile actor with potentially disastrous consequences. The supply chain certainly includes software, both that is obtained directly and that is embedded in components (which the purchaser of the component might not even know is there). But supply chain also includes physical components, and physical components of the components, that a contractor obtains from others. A physical component that is defective or is preset to degrade prematurely is every bit as much of a security threat as software that reports back to an adversary. Thus, we will use the term supply chain to refer to every component entering into a final product, whether it is hardware or software.[2]

Supply chain challenges

In September of this year, an interagency task force spearheaded by the DoD issued a report on "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States."[3] That report included an extensive appendix assessing traditional defense manufacturing sectors (e.g., aircraft, nuclear weapons, and shipbuilding) as well as crosscutting manufacturing sectors (e.g., electronics, machine tools, materials, and organics). The picture that emerges from that comprehensive report is that the defense industry is dependent on a global supply chain for many critical components, and achieving a reduction in that dependence will be difficult and will take substantial time. The reasons are varied, depending on the sector, but there are many common themes: Defense-specific manufacturing, though sizable, represents a relatively small part of many critical markets, and the private sector has been pursuing offshoring to keep costs as low as possible; there is a shortage of technically trained workers in the United States; and the technical capabilities of manufacturers, even in low-wage countries, have caught up to domestic manufacturers in many cases, leading to the withering of some U.S. capabilities.

While long-range approaches to address these and other issues are necessary, how should the federal government address supply chain security challenges today? And what are the long-range approaches that need to be pursued?

Possible approaches to reducing supply chain risk

One tempting approach would be to prohibit defense contractors from relying on supply chains that depend on manufacturers located in countries that, according to government intelligence, pose the greatest concern. Given the nature of the existing supply chain, such a one-size-fits-all approach is totally unrealistic. Where the risks of a compromised component are highest and the need for assurance of integrity the greatest, prohibiting reliance on a particular component might be prudent.

A robust testing capability that could determine a component's integrity may be effective if the testing could be done at scale and at a reasonable cost. Of course, cost considerations should be less of a constraint for more critical components of the national defense system. For example, the ability to test the integrity of components critical to the accuracy of anti-ballistic missiles would be worth almost any cost. If an adversary knew it had the ability to degrade the accuracy of the nation's anti-ballistic missile fleet, the existence of that fleet would lose its deterrent value, and the risk of nuclear attack would be significantly greater. Therefore, the ability to detect and counter an adversary's ability to degrade the accuracy of anti-ballistic missiles would be worth virtually any cost.

The core of any effective program to achieve supply chain integrity will be information sharing – sharing among the federal government's intelligence agencies, purchasers of defense equipment, and manufacturers of defense equipment. There must be a whole-of-government approach; what one part of the federal government learns must be immediately available to every other part of the federal government, and whatever actionable information the government obtains should be shared with appropriate industry actors. By actionable information, we mean only the information that a defense contractor needs to take actions necessary to protect its supply chain. That information might be, for example, that specific software should not be embedded in any defense equipment, or that such software should not be used on any computer that contains or processes any nonpublic design information.

This raises difficult questions about the impact of actionable information on U.S. entities. Would the actionable information shared with government procurement officials or defense contractors amount to a de facto debarment? What regulatory, statutory, or even constitutional requirements would apply? Would there be a due process right for an affected party to challenge the basis for the government's action, and if so what information would have to be made available? How can there be assurance that the actionable information is well-based and that there are no less severe options that could equally ensure supply chain integrity?

A second set of difficult questions relates to the extent contractors are going to be required to take actions on their own, not merely following direction from the government through actionable information. The implementation of procedures to ensure that each contractor knows what companies are in the full supply chain – not just who its own direct suppliers are but who are the suppliers to those suppliers, and so on – is a possible requirement. It has been reported that the DoD has launched a pilot program with a major defense contractor to put such a disclosure program in place.[4] Contractors know who their suppliers are, but they do not necessarily know who their suppliers' suppliers are, and that information might be competitively sensitive. Indeed, a supplier's web of suppliers might be the critical value that the supplier brings to the project, and being required to reveal that information to its customer might diminish or even eliminate the value that the supplier brings.

An interesting concept under consideration is requiring contractors to provide an "ingredients list" of the software embedded in their products,[5] but the question that remains is what would the government do with such information? Would the government itself do a risk analysis? Would more aggressive testing be required depending on the risk profile, and who would do such testing? And what would be the basis for any such risk analysis? The Israeli government is developing a variant of this approach, which requires owners of critical infrastructure and government agencies to purchase information technology (IT) services and products only from certified suppliers. The Israeli certification process will reportedly rely on a combination of self-certification of compliance with certain standards (which are not yet available in English) and third-party audits.[6] The Federal Acquisition Supply Chain Security Act of 2018, S. 3085, now pending in Congress, would make the federal agency acquiring a "covered article" responsible for assessing the supply chain risk "consistent with the standards, guidelines, and practices" to be identified by the Federal Acquisition Security Council to be established under the act.

Allocating the cost of protecting the supply chain

The matter of cost and who is to bear the cost are also critical considerations. To the extent that any requirements or new procedures are imposed with respect to existing contracts, there is a very strong argument that the government should bear all the costs, whether those costs are for the implementation of required procedures or, more controversially, the costs of having to find and pay the incremental costs associated with alternate suppliers. However, requiring the government to incur such costs will likely be controversial. Some will argue that the contractor has an existing obligation to provide a product that is suitable for the intended use, and a product that is not secure is not suitable for such intended use. Others will argue that the pricing of the contract was based on the requirements applicable when the contract was executed and that all additional costs resulting from a change in requirements should be paid by the government. This issue is likely to arise sooner rather than later because a DoD-wide audit launched last December is examining cybersecurity issues in the business systems used by the department. According to DoD's Comptroller David Norquist,

> "If you fielded one of those systems that is vulnerable to cyber intrusions, that is filled with errors in the way it is set up, we need to talk because you're one of the reasons we're not passing the audit, and we need you to fix it."[7]

For new contracts, all costs related to enhanced supply chain integrity procedures could be assigned to the contractor but there is an open question about whether requiring contractors to bear all such costs is the best policy. Increased costs related to implementing procedural requirements should be borne by the contractor and reflected in the offer price. But if the contractor must also pay the incremental costs of changing suppliers due to security concerns that arise after the contract has been entered, the contractor might be less quick to report suspicions about a given supplier. Further, when the bearer of the cost and the recipient of the benefit are joined, there is a party in a position to determine whether the benefits justify the costs, ensuring that total societal costs do not exceed the benefits. When any incremental security achievable by requiring an alternative supplier is to be paid for by a contractor unable to build that cost into its contract with the government, there is no assurance that the incremental costs do not exceed, and possibly greatly exceed, the incremental benefit.

Whoever is to bear the costs of alternative suppliers, it is essential that there be alternative suppliers that would be reliably secure – and that is not clearly the case today. This is a long-range issue that needs to be addressed. The Electronics Resurgence Initiative under the Defense Advanced Research Projects Agency is a piece of the long-range response, as well as many other efforts scattered throughout the government. These positive parts of the supply chain security effort are intended to ensure that there are secure domestic suppliers of leading-edge electronics, but as the Defense Security Service (DSS) has pointed out, the "majority of microelectronics in sustainment are obsolete" and a "large percentage of parts in acquisition are obsolete or will be within a year."[8] Having reliably secure sources of cutting-edge microelectronics is important, but it is not enough. There must also be reliably secure sources of obsolete microelectronics, and right now the government is overwhelmingly dependent on foreign sources for such parts in what the DSS refers to as a "gray market." As the DSS has noted, "DoD reliance on gray market + Limited ability to track semiconductors in the supply chain + Foreign ability to reverse engineer obsolete components that the DoD purchases = Critical risk."[9]

Conclusion

The attention generated by the Deliver Uncompromised initiative has sparked a critically important dialogue among government agencies, industry, and Congress. The challenges to reaching a sound balance that addresses supply chain integrity without breaking the country's procurement system are very difficult, but the failure to act is simply not an option if we wish to protect national security. In recognition of the risk, Secretary of Defense Mattis issued a memorandum on October 24, 2018, declaring that "[t]he impacts of the loss of intellectual property and data cannot be overstated – we must move out to protect our resources and our forces." To that end, Secretary Mattis has directed the stand-up of the Protecting Critical Technology Task Force and directed that it start two "sprints" – one of 30 days and one of 90 days, with work continuing beyond that as well. The sprints underscore the urgency of putting better protections in place.

The attention to supply chain vulnerability and to security generally can be a positive for those contractors willing to act proactively to address these issues. Having a program in place, being able to document the workings of that program, and being able to demonstrate that the program meets the highest standards available for protecting supply chain integrity should give contractors a competitive advantage in any competition for a DoD contract. In addition, having a quality program in place can protect the contractor from a fraud claim under the False Claims Act (FCA).[10] Further, having such a program in place should minimize the contractor's vulnerability to loss of its intellectual property. Any such program should be developed carefully with legal advice, to ensure that it creates these benefits and does not in fact increase the risk of an FCA fraud claim.

No discussion of supply chain integrity would be complete without mention of the report released by the MITRE Corp. examining the DoD's initiative, entitled "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War" (report).[11] The purpose of the report was to provide input in the form of 15 courses of action (COA) that support the formation of a "holistic strategy for dealing with supply chain security" within DoD. A brief discussion of each of those recommendations is appended to this paper.

Authors and contacts

Michael Mason
Partner, ADG Industry Sector Lead
Washington, D.C.
T +1 202 637 5499
mike.mason@hoganlovells.com

Robert Taylor
Senior Counsel
Washington, D.C.
T +1 202 637 5657
bob.taylor@hoganlovells.com

Stacy Hadeka
Senior Associate
Washington, D.C.
T +1 202 637 3678
stacy.hadeka@hoganlovells.com

Michael Scheimer
Senior Associate
Washington, D.C.
T +1 202 637 6584
michael.scheimer@hoganlovells.com

William Kirkwood
Associate
Washington, D.C.
T +1 202 637 3675
william.kirkwood@hoganlovells.com

Rebecca Umhofer
Professional Support Lawyer
Washington, D.C.
T +1 202 637 6939
rebecca.umhofer@hoganlovells.com

Endnotes

1 Rick Weber, *Senior DOD official questions cybersecurity 'pillar' for acquisitions as laid out in MITRE report*, Inside Cybersecurity (23 Oct. 2018), available here.

2 The Federal Acquisition Supply Chain Security Act of 2018, S. 3085, now pending in Congress, prioritizes the acquisition of a "covered article," which is defined as "information technology"; telecommunications equipment or services; the processing of information on an information system; or hardware, systems, devices, software, or services that include embedded or incidental information technology. Section 3(a), *adding* 41 USC § 4713(k)(2). This is broader than software, but narrower than every component entering into a final product.

3 Interagency Task Force in Fulfillment of Executive Order 13806, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States* (September 2018), available here.

4 Justin Lynch, *Pentagon Moves to Secure Supply Chain From Foreign Hackers*, Fifth Domain (21 Oct. 2018), available here.

5 Scott Maucione, *DoD, Commerce Consider Requiring 'Ingredients List' of Software to Protect Supply Chain*, Federal News Network (23 Oct. 2018), available here.

6 Rick Weber, *Israel to Mandate 'Certification' in Securing Supply Chain for Government, Critical Industries*, Inside Cybersecurity (8 Nov. 2018), available here.

7 Joe Gould, *Pentagon's Big Audit Will Inspect for Cybersecurity Flaws, Comptroller Says*, Fifth Domain (29 Oct. 2018), available here.

8 Defense Security Service, "Microelectronics Supply Chain Illumination," presentation at 2017 Microelectronics Integrity Meeting.

9 *Id.*

10 Cyber vulnerabilities could form the basis of a claim for fraud under the FCA premised on a contractor's representations about the suitability of the product or service for its intended use, or that appropriate procedures were followed to ensure that the product or service was free from flaws. If, for example, a contractor knowingly misrepresents the procedures it followed to protect its product or service from cyber vulnerabilities, the contractor could face liability under the FCA.

11 The MITRE Corp., Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War (Aug. 2018), available here.

APPENDIX

Discussion of the MITRE Corporation Report Courses of

1. Elevate security as a primary metric in DoD acquisition and sustainment

This focuses on the importance of security considerations in both the acquisition of and the sustainment of programs, in addition to the traditional considerations of cost, schedule, and performance objectives. The recommended mechanism is to add a "fourth pillar" for security in the acquisition and sustainment phases of the contract lifecycle, without compromising the traditional considerations of cost, schedule, and performance. The report suggests the fourth pillar should be evaluated by three parties: by government, by an independent third party, and by the contractor.

The report suggests that there is presently a "misalignment of risk and reward during acquisition" that results in risk, and the corresponding need for its resolution, being passed to a program's operational stages. Accordingly, a two-pronged solution — formal evaluation of security during the acquisition stage, and measurement and broad monitoring of security at the operational stage — is necessary.

During the acquisition stage, the report suggests that, among other things, an independently administered Security Index Score could be recognized and included in all evaluations of bidder and supply chain qualifications, to be reflected in decisions for selection and award.

ADG insight

Elevating security as a primary metric could increase the speed at which security issues are addressed. Nevertheless, deciding on useable metric(s) for measuring security may prove challenging. Such a metric will need to differentiate between security plans that a contractor has put in place, and the effectiveness of such plans. Likewise, a system for measuring security will need to ensure that contractors are properly motivated to disclose vulnerabilities rather than obscure them. Moreover, the plan for evaluating such metrics will need to clearly identify the attributes that will contribute to scoring, to ensure fair evaluation. As with other scoring methodologies in use today, such as for measuring past performance, scoring for security will need to include mechanisms for contractors to challenge unfavorable scores.

2. Form a whole-of-government National Supply Chain Intelligence Center

The report recommends the creation of a National Supply Chain Intelligence Center (NSIC) that would mirror that National Counterterrorism Center, created after 11 September 2001. The goal of this new center would be to "support the delivery to operating forces of warfighting capabilities that are uncompromised and resilient" through improved intelligence. The NSIC would resolve problems associated with existing stovepipe efforts to address security risks, including incomplete awareness of and information relating to existing threats. It would do this by creating an organization and function that would aggregate broad threat data collected first from DoD and the Intelligence Community, and ultimately from the whole government.

The NSIC would report to the director of national intelligence, the under secretary of defense for intelligence, and the National Counterintelligence and Security Center. The organization would have authority to communicate warnings of threats and actionable intelligence throughout the DoD and other U.S. government entities. Experts would be employed by the NSIC, charged with a broad understanding of government systems, vulnerabilities, and threats, as well as with comprehensively responding to such threats.

ADG insight

A mechanism for improving efforts within the U.S. government to understand, warn of, and respond to security vulnerabilities and threats, is an idea worthy of serious consideration and pursuit. The details associated with such efforts will require close scrutiny. Establishing a balance between a comprehensive method for effectively addressing vulnerabilities and threats with due process considerations may be chief among the concerns that contractors have with any new centralized functionality. Contractors or suppliers that are falsely identified as potential threats will need a mechanism to speedily appeal. Such allegations must be handled with great care and confidentiality because the potential for reputational harm based on false allegations may be devastating to any company. Based on this potential for harm, we recommend that industry representatives be involved in crafting the plans for implementing the NSIC and, in particular, the mechanism instituted to protect

industry. Integration of this COA with rules providing for due process protections should be considered.

3. Execute a campaign for education, awareness, and ownership of supply chain and digital risk

This advocates for better access to information, education, and training for program executives and acquisition workforce. It would help them to grasp the degree of, and rate of change in the asymmetrical threats faced by the United States. Accordingly, all personnel supporting the government in this area must understand and own the problem in order to properly respond to it. The report applies this view to the "entire acquisition and sustainment community," which therefore involves both the government and contractor communities. The report proposes that the human element in this community contributes to risk in the supply chain. The report suggests that inattention by senior executives within government and industry caused by insufficient understanding of this issue, yields inadequate investment in solutions.

ADG insight

Efforts to improve education and awareness may add substantial value. The key in determining the value of such education will depend on how well the educational program is developed and implemented. We suggest considering a system of certifications and continual professional education requirements that can be developed for supply chain security that are then made available to government and industry personnel. Such a system, if appropriately developed and implemented, could validate how well the curriculum is adopted, as well as provide a potential measure to qualify employees for advancement, and suppliers for awards.

4. Identify and empower a chain of command for supply chain with accountability for integrity to Deputy Secretary of Defense

In recognition of the broad overarching nature of the risk to the supply chain, this proposes that an empowered command with appropriate authority to reconcile and manage the diverse inputs that go into supply chain decisions (e.g. from acquisition, security, and those related to development, requirements definition, acceptance, and the like) is necessary. The report proposes that service component vice chiefs should be made responsible for the integrity of the supply chain for each command, and that inter-service supply chain matters should be addressed by the "Vice Chairman, Joint Staff, and possibly an accountable Supply Chain Integrity Executive within the Office of the Secretary of Defense." Each would consequently have authority for overseeing and directing the protection of its entire supply chain and for coordinating such protection, as necessary, with the whole of government.

ADG insight

An empowered supply chain of command is a good suggestion. It will help improve communication and effectiveness of government, particularly in the identification of and mitigation of supply chain risks and, accordingly will help maintain the integrity of the supply chain. We suggest that such infrastructure be developed with not only the integrity of the supply chain in mind, but also with the protection of individual suppliers in mind. This is to avoid the potential for creating a de facto debarment system without due process through, in this instance, an integrated supply chain command that can identify and broadly avoid members of the industrial base that it believes are a risk. Such a risk to individuals in the supply chain may discourage suppliers from sharing information related to supply chain risk, for fear that the sharing of risk may result in competitive harm to the supplier. Integration with rules providing for due process protections should be considered.

5. Centralize SCRM-TAC under DSS and extend DSS authority

Another structural recommendation for the government suggests that the Supply Chain Risk Management Threat Assessment Center (SCRM-TAC) should report to the Defense Security Service (DSS). The report asserts that this change is necessary to broaden and make more scalable the capabilities of SCRM-TAC, which today reports on the capability and intent of adversaries, but not on the vulnerabilities and consequences for each component.

ADG insight

We believe that integration of SCRM-TAC with DSS presents a good opportunity for enhanced communication and effectiveness in government. As discussed in the preceding point, however, there are significant risks to individual suppliers of being harmed by false or incomplete information.

6. Increase DoD leadership recognition and awareness of asymmetric warfare via blended operations

This examines the problems associated with the "largely unrecognized" impact of asymmetric warfare. The suggestion is that the nation lacks comprehensive deterrence against asymmetric actions. The report recommends that the same degree of focus and diligence that would be used to address a kinetic attack on the

United States, be duplicated in the area of asymmetric threats. As previously discussed, there is a need for education and understanding among DoD leadership so that they perceive and adjust to our enemy's intent to attack "through all of the supply chain (hardware, software, and service), cyber IT, cyber-physical, and the human element (witting or unwitting)."

ADG insight

Efforts to increase awareness of the threat posed by asymmetric warfare should be encouraged. Increasing industry's awareness of the threat should also be considered, in order to ensure industry's cooperation and commitment to the measures necessary to better improve security.

7. Establish independently implemented automated assessment and continuous monitoring of DIB software

This addresses software security and risk, based on the view that all forms of software — custom developed, commercial, and open source — are subject to potential compromise by adversaries who may add malicious code to software. This "malicious functionality" may be added by developers in the supply chain who may purposefully corrupt one or more components of the complete software build. Such threats carry a risk of immediate and/or latent harms that can be triggered on-demand. As a result, static assessment and certification is not sufficient. This proposes that tools and possibly independent organizations should be developed to automatically validate software and continuously monitor for "nefarious behavior" in order to identify and counteract such threats as they emerge.

ADG insight

A tool that can be used to reliably validate, monitor, and measure the risk of compromised software would be useful, as would an independent methodology and rating organization. It would be important to define where such measurements and monitoring are established in the acquisition lifecycle. For example, will such measures and monitors be evaluated in the acquisition stage, the sustainment stage, or both? Further, it will be important to ensure that such tools do not act to impede the discovery or disclosure of software vulnerabilities. This could happen if developers or governmental entities rely too heavily on tools that are unreasonably expected to identify and disclose every possible concern. Moreover, savvy developers in the supply chain could hide compromises in software by learning to evade the triggers and flags that are used by monitoring tools to detect compromised software.

8. Advocate for litigation reform and liability protection

This suggests that the threat of litigation and legal liability can incentivize positive behaviors in the contractor community, particularly in the production of software. Annex II of the report suggests reducing litigation risk in some areas and increasing it in others. Among the suggestions for reduced liability are: (1) the expanded availability of safe harbors that will encourage contractors to share "suspicious or potentially derogatory information" with less risk to the organization; and (2) use of the designation "trusted supplier" that is accompanied by higher reporting responsibilities, and extended protections under the Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY). This suggests that increased liability should be explored in situations in which a contractor fails to take reasonable and timely cyber and supply chain assurance measures, or in which a contractor does not take reasonable and responsible actions based on known threats, vulnerabilities, and risks.

ADG insight

Efforts to improve the early discovery of software vulnerabilities should be explored. Accomplishing such efforts through litigation reform must be approached carefully to ensure that contractors are encouraged to reveal vulnerabilities and other issues with software. Additionally, such efforts must be balanced against the potential impact that incentives and penalties may have on innovation and the industrial base. Too much risk placed on suppliers may force software developers to exit the government supply chain.

9. Ensure supplier security and use contract terms

This suggests moving beyond minimum standard compliances toward using incentives for companies to examine and improve practices and systems on a continuous basis. Discussed further in Annex III of the report, this suggests the need to address the entire supply chain, including suppliers of commercial off-the-shelf equipment, when pursuing a secure and resilient supply chain. Annex III reviews suggestions for ensuring readiness of the supply chain to respond to additional security requirements, and discusses the use of contract terms and other contract requirements to help encourage suppliers to improve security.

The report acknowledges that change must be pursued carefully, so as to not overwhelm the industrial base or interfere with innovation. Additionally, the report suggests that the DoD should work with prime contractors to help less capable suppliers improve security capabilities. This could be done by moving information system and application platforms to qualified secure cloud platforms. Other suggestions are provided, including revising DoD Instruction 5000.02 and Defense Acquisition Guidance to increase the importance of supply chain and software assurance, adding further emphasis in acquisition planning stages (and requisite funding) to increase security requirements, place increased emphasis on the provision of system security plans, and highlighting security as a competitive discriminator.

ADG insight

As with other aspects of the report, we believe that an effort to broadly move suppliers from a focus on compliance to a commitment to continual improvement in security would be helpful. We agree with the report that such efforts must be tailored and monitored carefully, so as to not interfere with innovation.

10. Extend the 2015 National Defense Authorization Act (NDAA) Section 841 authorities for "Never Contract with the Enemy"

This addresses the unique supply chain, acquisition, and operational needs of forward-deployed combatant commands. These unique requirements, together with the hostile and high counterintelligence environments in which they often operate, heighten the importance of the assistance these commands need. This supports the formation of the NSIC, discussed earlier, in order to help these commands. The full remedy suggested is in legislation drafted by DoD that further modifies Sections 841-843 of the 2012 NDAA, which was earlier modified by the 2015 NDAA. These modifications, discussed in Annex IV of the report, would both strengthen and extend these provisions so that they more completely address supply chain issues encountered by forward-deployed combatant commands.

ADG insight

This is an internal goal for the government that we believe should be pursued. As discussed elsewhere, we believe that it is important to involve the contractor community in the evaluation of measures to monitor and protect the supply chain for forward-deployed combatant commands, to ensure that the least invasive measures are used to achieve supply chain integrity and resilience, so that suppliers aren't subjected to blacklisting without due process, and delivery of components to these commands is not slowed or otherwise impeded. Integration with rules for providing for due process protections should be considered.

11. Institute innovative protection of DoD system design and operational information

This addresses the protection of information relating to programs and systems, such as "system design, trades, vendors, parts lists, operational details, etc." It observes that because of confusion over classification of such information, "vast amounts" of this information is available to the general public. It suggests modeling protection measures after certain aspects of how the commercial world protects its IP, including strict controls relating to how information is shared and with whom. Among the suggestions offered is the use of technologies to share e.g., system design information for only as long as needed (though it is hard to imagine this measure thwarting the efforts of a sophisticated adversary). Ultimately, the DoD could do better in protecting programs throughout their lifecycles, with an emphasis on protecting programs in early stages of the lifecycle, in order to make it harder for adversaries to truly understand the technical and operational parameters associated with such programs.

ADG insight

Efforts to raise awareness of and combat risks to the supply chain should be a priority for the government. In particular, mechanisms for limiting the disclosure of system design information in order to make it more difficult for such information to make its way into enemy hands should be examined carefully. The government as well as the supply chain will need clear instructions regarding what types of information must be protected and how this is to be done. Moreover, the government will need to balance the risk of information getting into enemy hands, with the risk that incumbents may become embedded in the government's supply chain due to the inability of new suppliers to gain access to information critical to their ability to effectively compete.

12. Institute industry-standard IT practices in all software developments

This addresses the composition of various components of software, with suggestions that due to the varied and complex supply chain associated with today's software, little is known of the pedigree and provenance of the end product. Suggestions include the promotion of a software bill of materials that identifies the provenance of the components of the end software product, together with other mechanisms to continually monitor implemented

software to identify anomalies in, and other events affecting the operational system. Additionally, it suggests that the composition of software purchased by the government, should be tracked by suppliers and that such tracking and disclosure of software composition should be mandated through use of contractual terms, with liability for damages and other sanctions available to address suppliers who knowingly supply false information.

ADG insight

As stated elsewhere, it is important to ensure that such tracking and disclosure requirements do not overburden the supply chain. Additionally, as mentioned previously regarding the over-reliance on monitoring tools, it is important that steps taken do not result in a false sense of security. Understanding the pedigree of software is not the equivalent of ensuring its integrity. Integration with existing rules relating to country of origin such as the Buy American Act, Trade Agreements Act, and Defense Security Cooperation Agency guidelines for foreign military financing, must also be considered when pursuing this course.

13. Require vulnerability monitoring, coordinating, and sharing across the chain of command for supply chain

In a return to a recommendation found elsewhere in the report, this recommends a requirement for vulnerability monitoring, coordination and sharing among each service component in its acquisition and sustainment efforts. This identifies current monitoring efforts as limited to cleared facilities. Ultimately, it concludes that a vendor vetting database might ultimately be created that would be used by various components in order to track and communicate supply chain risks.

ADG insight

The goal of sharing information within the government regarding vulnerabilities in the supply chain is a worthy one. We have concerns regarding how a vendor vetting database might be used, and what due process protections suppliers may have when they, rightly or wrongly, end up listed in such a database with negative information listings. Integration with rules that provide for due process protections should be considered.

14. Advocate for tax incentives and private insurance initiatives

This advocates for the use of tax incentives and private insurance initiatives to incentivize suppliers to "embrace cyber and supply chain security." The report suggests that if contractors can be incentivized to embrace security in such a way that converts the pursuit of security measures from a cost issue to one that generates profit to the supplier, a multifold benefit will result: contractor intellectual property (IP) would be protected, as would DoD technical data and other sensitive but unclassified information.

ADG insight

Tax incentives might be a useful tool to encourage implementation of supply chain integrity measures throughout the economy, and not just by companies within the Defense Industrial Base. Given the increased reliance on commercial products as part of the supply chain, broad implementation of protective measures might be necessary to ensure national security. This could have collateral benefits in reducing the theft of intellectual property estimated to cost the U.S. economy as much as US$600 billion per year. As the authors of the report suggest, this goal may take some time to achieve.

15. For resilience, employ failsafe mechanisms to backstop mission assurance

This discusses contingency plans or "fail safes" developed to provide alternatives to enable the DoD to complete a mission. Such plans should be independent of specific software and/or other components of the supply chain, according to the report. The report offers examples from the commercial sector that the DoD should follow in order to ensure that the ultimate mission, even if hampered, can be successfully accomplished.

ADG insight

A goal of resilience in the government's ability to deliver missions seems to be an obvious and worthwhile goal for the government to pursue. Cost may be an initial constraint, but from the perspective of total cost of ownership, it may be that the purchase of resilient systems for key missions may ultimately be a lower cost solution. Such requirements for resilience, where they involve the supply chain, should be specified as a requirement in the solicitation and resulting contract so that the government and industry can both benefit from maximum competition. Additionally, expedited moves by government to resilient systems, such as cloud platforms, may lessen the cost for resilience in the long run.

Hogan Lovells

Aerospace, Defense, and Government Services Industry

We can help you anticipate and deal with the risks before they become problems.

The aerospace, defense, and government services (ADG) industry is changing significantly. Global spending on defense and weapon system platforms is increasing. Governments are procuring analysis and engineering services to address escalating terrorism threats, cybersecurity concerns, and an ever-increasing demand for big data analytics. Commercial space and unmanned vehicle advances have invigorated key sections of the industry. Brexit and the administration change in the U.S. are creating challenges and opportunities across the globe. And, technological advances such as 3-D printing are creating unique opportunities for innovative products, decreased time-to-market schedules, and agile maintenance and repair services.

Our clients demand experience. They need comprehensive and cost-effective support from lawyers who know their business and understand the demands of their industry.

That's where we come in.

Be ready

Our global ADG practice is focused specifically on your needs. Our team includes industry-leading lawyers with corporate, commercial, regulatory, investigations, and litigation experience. We work closely with some of the largest and most established ADG companies in the United States, Europe, and Asia. We advise dozens of middle market businesses, emerging companies, new ventures, global entities, along with investment banks and private equity firms that are active in the industry.

We know, because we've been there

Our clients are also some of the most innovative in the world. They build manned and unmanned aircraft, supply parts, and materials to the aerospace industry, and develop and deliver the technologies essential to defense and national security. Our clients make and provide launch vehicle and satellite services and provide the services and innovations required for homeland security and critical governmental operations.

So let's work together

Together we will tackle the difficult challenges, capitalizing on opportunities, and avoiding pitfalls. We will guide you through government regulatory and procurement hazards and protect your interests in disputes and government investigations. Our industry focus enables us to fully understand your business and the challenges you face. We anticipate emerging issues before they become a problem and we give advice that achieves results.

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com