wiley

NEWSLETTER

MITRE Report Recommends Critical Changes to Supply Chain Security

September 2018

In August 2018, MITRE Corporation released a report recommending significant enterprise-wide changes to cyber and supply chain security, including changes in the role of cybersecurity in the procurement process. The report, "Deliver Uncompromised, A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War," is the latest cybersecurity development for defense contractors, and a sign of further changes to come.

The "Deliver Uncompromised" MITRE Report

The genesis of the MITRE report dates to 2010, when government officials and industry executives began publicly discussing concerns about the federal Government's tolerance for contractors who repeatedly delivered "compromised" capabilities to the DOD and Intelligence Community (IC). The report states that many DOD agencies and programs have already been compromised. MITRE's study focused initially on software integrity, but widened to include supply chain security, including major weapon systems. The report highlights the changing character of war, as adversaries strategically shift the paradigm in which they engage the United States from traditional kinetic actions to non-kinetic blended operations that take place in the supply chain, cyber, and human intelligence domains. Adversaries avoid fighting in areas of traditional U.S. strength, and seek to exploit asymmetric capabilities to defeat technological advances. This asymmetric engagement requires careful consideration of supply chain security and cybersecurity for DOD and its contractors.

The stated objective of the "Deliver Uncompromised" report is to "deliver warfighting capabilities to Operating Forces without their critical information and/or technology being wittingly or unwittingly

Practice Areas

Government Contracts

lost, stolen, denied, degraded, or inappropriately given away or sold." The report acknowledges several structural challenges to achieving this objective. Notably, the report alleges that "overreliance on 'trust,' in dealing with contractors . . . has encouraged a compliance-oriented approach to security—doing just enough to meet the 'minimum' while doubting that sufficiency will ever be evaluated." The report recommends a fundamental change from the current trust-based system to one based on compliance with expert, independent industry standards.

The report recommends that "product integrity, data security, and supply chain assurance should become ***key contract award criteria***." To that end, the report recommends a number of significant Courses of Action (COA), including several that, if implemented, would have considerable impact on government contractors. The first and most significant COA would be to elevate security to a "primary metric" in DOD acquisition and sustainment. As the report explained, DOD currently measures program success and competitiveness largely using a set of well-established cost, schedule, and performance objectives. These acquisition parameters, however, fail to account for the true cost and risk of capability ownership, including system integrity and mission assurance, of which supply chain and cybersecurity are key components. The report calls for security to be recognized as a fourth pillar in the acquisition process, and envisions security evaluations taking place in three dimensions: by the Government on contractors currently performing on other contracts; by an independent entity that will prepare and make available System Integrity Scores (SIS), akin to the "Moody's" model; and by privately procured monitoring services. The report places considerable emphasis on the role of the SIS, which is envisioned as a public-private entity that could act as an accrediting intermediary, and whose ratings could be used to qualify and evaluate offerors in the source selection process. These changes, according to the report, should incentivize contractors to invest more heavily in cyber and supply chain security. Relatedly, the report recommends reducing some of the transparency in acquisitions, particularly in acquisitions of high-impact programs and in areas with heightened cyber and supply chain risk, on the basis that "massive amounts" of information regarding these programs has been exposed to and exploited by adversaries.

If these changes are implemented, they will likely create new urgency for successfully demonstrating compliance with existing security standards, such as those required in DFARS clause 252.204-7012 and outlined in NIST SP 800-171, in addition to demonstrating strengths beyond the minimal levels of acceptability. Since the report envisions broader government review and assessment of DFARS 252.204-7012 compliance, it may pave the way for compliance audits and enforcement actions. And, to the extent that cyber and supply chain security become more prevalent in the source selection process, contractors can expect to see these issues explored more frequently in bid protest litigation.

The report contains several other recommended COAs. For example, it recommends the creation of a jointly-governed inter-agency entity, called the National Supply Chain Intelligence Center, which can aggregate and analyze disparate data and disseminate reports to at-risk industry partners. The report recommends requiring the application of automated validating tools and software to conduct independent continuous monitoring for nefarious behavior. The report also calls for DOD to spearhead advocacy efforts for litigation reform and liability protection for contractors, especially for those involved in software development. The report

acknowledged that contractors often hesitate to share relevant threat information with the Government out of concern that they could expose themselves to liability, in part because the Government may be unable to protect the contractor's identity or the information it provides. The report also raised the possibility that companies designated as "trusted suppliers" would be required to agree to a greater set of disclosure obligations and information sharing. Finally, the report acknowledges that smaller subcontractors who are deeper in the supply chain are more likely to be attractive targets for hostile actors, but they may lack the resources to properly defend themselves. To mitigate that risk, the report recommends tax incentives, akin to those provided to businesses that invest in renewable energy, and private insurance initiatives to spur development for smaller companies.

In summary, the MITRE report contains several significant and wide-ranging proposals for changes to the role of cybersecurity in government acquisition and administration of contracts. While it remains to be seen which changes will be implemented, these proposals establish a roadmap for an increasingly significant role that cybersecurity and supply chain security will play for federal contractors.