ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Deliver Uncompromised

Pentagon Leadership Can Improve Supply Chain Security Across the Nation

September 2018

Authored by:

Parham Eftekhari, Executive Director, Institute for Critical Infrastructure Technology

Drew Spaniel, Lead Researcher, Institute for Critical Infrastructure Technology

Deliver Uncompromised

Pentagon Leadership Can Improve Supply Chain Security Across the Nation

September 2018

Authored by

Parham Eftekhari, Executive Director, Institute for Critical Infrastructure Technology

Drew Spaniel, Lead Researcher, Institute for Critical Infrastructure Technology

---

ICIT Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Support ICIT

Through objective research, publications and educational initiatives, the Institute for Critical Infrastructure Technology, a 501(c)(3) cybersecurity think tank located in Washington, D.C., is arming public and private sector leaders with the raw, unfiltered insights needed to defend our critical infrastructures from advanced persistent threats, including cyber criminals, nation states, and cyber terrorists.

Our mission is to cultivate a cybersecurity renaissance that will improve the resiliency of our Nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders.

Financial capital from generous individual and corporate donors is the lifeblood of the institute and a force multiplier to our efforts. With your support, ICIT can continue to empower policy makers, technology executives, and citizens with bleeding-edge research and lift the veil from hyper-evolving adversaries who operate in the dark.

Together, we will make quantum leaps in the resiliency of our critical infrastructures, the strength of our national security, and the protection of our personal information.

http://icitech.org/support-icit/

Contents

Introduction: Pentagon Leadership Can Abate Security-by-Design Apathy

There are events in history which pass with little fanfare that time later shows to have been moments of significant consequence to a cause, a society, or a Nation. The Pentagon's recent public declarations that cybersecurity will become "more and more of a discriminator" in the Department of Defenses' multi-billion dollar acquisition determinations is a precedent-setting evolution in policy which, while in its infancy and currently confined to the defense industrial base, has the potential to bring about change across a diverse range of critical infrastructure sectors around the Nation [1].

Part of the significance of the "Deliver Uncompromised" initiative is rooted in its clear assessment of the responsibility that the contractor community has in improving the resiliency of all warfighting capabilities. Its Courses of Action (COA) call on the government to reward contractors who are willing to meet higher standards and adhere to security-by-design practices with acquisition awards, and its authors astutely identify near and long-term objectives to account for the challenges of implementing their gargantuan vision.

While "Deliver Uncompromised" is designed to impact the defense industrial base, it may also be the spark that will change supply chain practices across multiple critical infrastructure sectors. Practically speaking, the defense industrial base is so massive that requirements for higher standards will certainly impact organizations who have a foot in multiple sectors. It is almost inconceivable to imagine that once an organization is forced to improve its cyber hygiene and development practices for its defense client(s), it would not extend those practices to clients in other sectors. Furthermore, the fact that the largest buyer on the planet is articulating, vocally and through its checkbook, that the pervasive culture of "deploy now, patch later" is unacceptable and will no longer be tolerated will no doubt have a ripple effect that will inspire others sector leaders to follow suit accordingly.

It is important to the authors of this paper that the reader understands that their support for this initiative does not equate to animosity or blame towards the vendor community. Security is a shared responsibility amongst all stakeholders, from the supply chain to the buyer. Cultural norms, good and bad, are developed over time, and while conversations to course-correct are difficult, they are done with the understanding that all parties have one interest in mind: the national security and resiliency of our country's critical infrastructure sectors.

"Deliver Uncompromised" Sends a Needed Message

Warfare has evolved into an asymmetric amalgamation of digital and kinetic vectors; primarily, supply chain, cyber-physical, cyber-IT, and human domain. Democracy, moral values, critical infrastructure information, and even the public perception of reality is targeted through the exploitation of vulnerabilities in hardware systems, software applications, and people's

characters. To combat the rise in threats ranging from sophisticated adversaries to insider threats to script kiddies, the Department of Defense recognizes that it must make better use of its existing resources to identify, protect, detect, respond to, and remediate network and supply chain threats. This requires a seismic shift in many cultural and policy areas to usher in an era of increased coordination with the Intelligence Community, increased cooperation with the Department of Homeland Security, improved accountability and relations with contractors, new security standards and best practices, changes to the acquisition process, and motivated stakeholders to adopt risk mitigation as a default strategy rather than a “business loss” or expense.

To better protect critical infrastructure and essential systems, the Pentagon recently announced that it might begin awarding contracts based on security assessments as well as cost and performance. The strategy, referred to as "Deliver Uncompromised," was developed by Mitre Corp. to ensure mission resilience by instituting a deliberate, inherent elevation of integrated risk management from concept through retirement of a project within the DoD and its contracting base and to directly address the DoD’s need to secure that innovation from compromise. One of the effects of “Deliver Uncompromised” will be to shift the culture of the supply chain beyond a position of security compliance. According to a Pentagon spokeswoman, Maj. Audricia Harris, "The department is examining ways to designate security as a metric within the acquisition process. Determinations [currently] are based on cost, schedule, and performance. The department's goal is to elevate security to be on par with cost, schedule, and performance."

According to the Mitre report proposing the strategy, “A modern aircraft may have more than 10 million lines of code. Combat systems of all types increasingly employ sensors, actuators and software-activated control devices” [2]. In fact, a Boeing 787 has 6.5 million lines behind its avionics and online support systems. The control software to run a U.S. military drone uses 3.5 million lines of code. The Google Chrome browser may run on as much as 6.7 million lines of code. All Google services combined allegedly use 2 billion lines of code.

Even using a very generous range of 0.003 to 0.08 vulnerabilities per thousand lines of code (LoC), we see that at any given time there are 3 to 80 exploitable vulnerabilities in every application per million (LoC). Threat actors only require one exploitable vulnerability in one application on one system to breach the network, infiltrate a system, establish a foothold, and then laterally move across the network via trusted connections onto more valuable and more secure systems by stealing credentials as they strategically transition.

Security is a complex stakeholder problem that requires the engagement and attention of all parties. Suppliers, whether from the defense industrial base or elsewhere in the private sector, are stakeholders that must act as responsible partners in defense of critical infrastructure

systems to which they provide applications or services. It is irresponsible for suppliers to shift risk and liability wholly onto public or private sector customers through service level agreements (SLAs) and terms and conditions, or to justify inadequate spending on product development because the organization's exposure is mitigated with cyber insurance policies that offset risk by estimating how many consumers might sue when a breach occurs.

By incorporating security into acquisition determinations, the Pentagon would be sending a clear message to top private sector firms that the "deploy now, patch later" culture of modern software developers and service providers needs to change so that consumers are no longer used as the crash test dummies of flawed and vulnerable products that are easily exploited by malicious adversaries following the path of least resistance into the network [2]. With this act, boardrooms around the Nation will stop categorizing security as a cost which should be minimized, but as a value-driver and business differentiator which deserve increased R&D budgets, proper placement on product development roadmaps, and ultimately, as a requisite for go-to-market strategies.

What is "Deliver Uncompromised"?

"Deliver Uncompromised" is a strategy proposed by Mitre to improve cyber and supply chain security of the Department of Defense and Intelligence Community through suggested courses of action that quantify risk, dismantle intra- and inter-government information silos, and prioritize threat mitigation. In effect, security is instituted as the fourth determinant of solution acquisition (alongside cost, schedule, and performance) and greater attention is dedicated toward the protection of operational security or software assurance [3] [4]. "Deliver Uncompromised" places emphasis on the security of systems, data, communications, supply chain, and information in general, regardless of medium or vehicle. In effect, contract deliverables must be provided in a state that is uncompromised by hacking, the inappropriate sharing of data, or contamination of the data throughout the entirety of the product lifecycle. During a June 21, 2018, hearing of the House Armed Services Committee, Anthony Schinella, national intelligence officer for military issues at the Office of the Director of National Intelligence stated, "We must have confidence that industry is delivering capabilities, technologies and weapon systems that are uncompromised by our adversaries, secure from cradle to grave. It is no longer sufficient only to consider cost, schedule and performance when acquiring defense capabilities. We must establish security as a fourth pillar in defense acquisition and, also, create incentives for industry to embrace security, not as a cost burden, but as a major factor in their competitiveness for U.S. government business" [5].

At its core, the "Deliver Uncompromised" proposal is a suggested renovation of the acquisition process. Mitre's proposal offers some courses of action to measure the security and

performance of vendor solutions. By adopting "Deliver Uncompromised," the Department of Defense will send a clear message to its suppliers that including security-by-design and operational continuity measures in vendor solutions are expected in future products; else, contracts, deals, and business will be ceded to firms that are willing to adapt to the realities of the evolving threat landscape and include inherent security at each layer of their product lifecycle. By adopting the strategy, the DoD will define, shape, and standardize the responsible conduct of its suppliers. Developing firms will thereafter emulate the responsible behavior of market leaders and incorporate internal layered security as a prerequisite to entering the public sector market. The DoD can define requirements to incorporate new security measures, publicize security research or effective incorporation strategies, reward superior security measures in the source selection process, including contract terms that impose security obligations, and use contractual oversight to monitor contractor accomplishments [3].

Impact on the Private Sector

The adoption of "Deliver Uncompromised" most directly impacts DoD contractors by increasing the requirements for security and supply chain management at all levels and throughout product lifecycles. By elevating the minimum standard for security prerequisite to work on any component of a DoD contract, the DoD shifts contractor focus from overhead costs to security as a differentiator for sustained business. Further, because contractors are responsible for any subcontractors it utilizes, the onus of assessing the security of each subcontractor falls onto contractors because their ability to conduct business with the DoD is at stake.

Since many market leaders and innovators rely on public sector contracts, the impact of an effective adoption and implementation of "Deliver Uncompromised" cannot be overstated. Even if "Deliver Uncompromised" is only implemented in part, it will be a success if in the short-term there is a measurable decrease in the number of security incidents that result from the lackadaisical cybersecurity and cyber-hygiene practices of prime contractors and subcontractors [4]. It will be a success in the long-term if other public sector entities and private sector firms begin to adopt its concepts and require security-by-design throughout the product lifecycle of vendor solutions according to NIST 800-160.

The potential behind "Deliver Uncompromised" derives from the influence that the Department of Defense and the Intelligence Community have over market leaders. The cybersecurity of public assets and citizens have too long been at the mercy of third-parties and vendor solutions that under-deliver on their promise of security and reliability. Until now, each breach is met with public apologies and promises of future remediation that amount to little more than words and moot actions. Retroactive mitigation and remediation measures are engaged when damage has already occurred, and an impact has already been realized. Until

now, the brunt of the negative consequences of vendor insecurity has fallen entirely onto the public and the public sector. Incentivizing proactive action through rewards has proven as ineffective as threatening punishments. “Deliver Uncompromised” proffers a realistic compromise that requires proactivity. Rather than offer rewards for what should already be included or threaten penalties or "if-an-incident happens" empty threats that can be ignored, subverted through legal clauses, or compensated with cyber-liability insurance, Mitre’s proposal prevents prime and subcontractors who are not compliant with security standards from winning business contracts in the first place.

“Deliver Uncompromised” and what will hopefully be many sector-specific derivatives redefines the client-vendor relationship. Buyers will expect inherent security. Marketable products will have to feature commensurate security. There will be no more middle ground for faux experts and silver-bullet solutions.

What the non-DoD sector Can Glean from “Deliver Uncompromised”

The “Deliver Uncompromised” proposal was created to address specific concerns for the Department of Defense and the IT components of its weapons systems. However, an analysis of the document and its 15 courses of action (Appendix A) yield actionable insights that both suppliers and buyers can leverage to begin to improve their resiliency and security posture immediately.

In this section, ICIT offers recommendations gleaned from the report for suppliers and buyers as a starting point for organizations looking to create their own culture of “Deliver Uncompromised.”

Recommendations for Buyers

Define Roles and Responsibilities

When roles, responsibilities, authority chains, and accountability are undefined within an organization or among stakeholders, operations become stunted, information becomes siloed, communication may be inhibited, parties may be begrudged, and decisive action may be significantly delayed beyond the point of timely response [3].

Quantify Risk

Security is paradoxical in that when it is working, nothing dramatic (aside from deeply technical indicators) can be observed; however, when security is insufficient or non-existent, incidents occur which result in impacts on consumers, reputational harm, monetary loss, and other negative outcomes. Rather than viewing security as an expense or a “business loss,” organizations should adapt to viewing it as a measurable quantity that increases the realistic

profit (by offsetting the inevitable losses of cyber-kinetic exploitations), that protects the systems and reputation of the organization, and that deters adversaries from future attacks. The first step in any security strategy is to conduct a risk assessment according to the Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), Factor Analysis of Information Risk (FAIR), the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF), or Threat Agent Risk Assessment (TARA) frameworks. By determining the organization's risk profile and threat appetite, it can make better informed decisions concerning solution acquisition. More importantly, it will be better equipped to assess the inherent security of vendor solutions according to the principles of "Deliver Uncompromised" and to ensure that the vendor offerings meet the needs of the organization.

Hold Partners Accountable

Security is a stakeholder problem and the entirety of liability and risk should not be shifted to the client. When considering vendor solutions, customers, who possess agency due to their market influence and buying power, should discuss the distribution of responsibility, liability, and any lingering risk.

Require Security-by-Design in Acquisitions

Buyers need to recognize in the modern dynamic market that the differentiators between innovators and emulators are minimized; consequently, substitute products exist for most solutions. As a result, if a vendor solution fails to include layered security-by-design, a consumer can instead purchase a comparable product that does incorporate security from one of that vendor's competitors. By leveraging their buying power, clients can collectively send a clear message that the future sales of vendor solutions depends as much on the inclusion of security as it does on cost, performance, and schedule.

Recommendations for Vendors

Apply NIST Frameworks Now

At the time of this writing, "Deliver Uncompromised" remains a proposal; however, it is inevitable that the DoD will set more robust minimal security requirements for vendors and their products. To be better prepared for changes in regulation, it is suggested that enterprising firms adopt industry standard frameworks such as NIST 800-53, NIST 800-171, and new frameworks such as NIST 800-160. Firms that already exceed the minimum requirements set in the near future (which will likely be derived from the aforementioned or similar standards) will have a significant market advantage over their competitors because their security posture will be more robust, mature, and in line with industry standard requirements [4].

Manage Subcontractors

Subcontractors can be the source of insider threats, lateral compromises, and other embarrassing security vulnerabilities. Contractors that wish to win and retain public sector contracts should ensure that any subcontractors they employ are likewise aligned with NIST and other industry frameworks [4].

Prepare for the Future Based on the Hyper-Evolving Threat Landscape

"Deliver Uncompromised" offers short, mid-range, and long-term courses of action across legislation and regulation, policy and administration, acquisition and oversight, programs and technology. Vendors should consider the recommendations of the proposal and adopt a similar mindset. A cybersecurity and cyber-hygiene renaissance is coming. Even if firms doubt that "Deliver Uncompromised" will be adopted, the National Defense Authorization Act recently passed with very similar themes. Firms that will be successful in the future will be those that establish policies, procedures, and implement controls to maintain security framework alignment, that appropriately invests resources in security, and that can quickly adapt to change. Security-by-design, continuous monitoring, layered security, a rigorous subcontractor selection process, and similar practices will be unparalleled market differentiators in the near future [4].

Conclusion

Mitre's "Deliver Uncompromised" recognizes the need for immediate action coupled with a long-term commitment and strategy to mitigate inherent security vulnerabilities and to course correct the asymmetric distribution of risk in the buyer-seller relationship, which currently transfers all liability and risk onto the unknowing and unaccepting buyer when in reality, the vendor should ensure that their product is secure and reliable prior to distribution. Shifting national cybersecurity culture is not trivial, and it will not be immediate. Cybersecurity and cyber-hygiene are complex multi-stakeholder issues without clear solutions to address the hyper-evolving threat landscape; however, Mitre's "Deliver Uncompromised" admirably recommends short-term, mid-range, and long-term courses of action that the Department of Defense, Intelligence Community, or any other firm can take to initialize the overdue cybersecurity and cyber-hygiene renaissance that prioritizes security as buyer-required and vendor-guaranteed. The report details flexible options that span legislation and regulation, policy and administration, acquisition and oversight, programs and technology. While the courses of action may not be adaptable for every firm in every sector, the fundamental principles within the proposal are universally applicable to the acquisition process and supply chain security of most firms [3].

ICIT Contact Information

Phone: 202-600-7250

E-mail: http://icitech.org/contactus/

ICIT Websites & Social Media

www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

Sources

[1] P. McLeary, "DoD, Industry Sparring Over New Cyber Rules, Ellen Lord Says", *Breaking Defense*, 2018. [Online]. Available: https://breakingdefense.com/2018/07/dod-industry-sparring-over-new-cyber-rules-official-says/. [Accessed: 04- Sep- 2018].

[2] Nissen, C., Gronager, J., Metzger, R. and Rishikof, H. (2018). *Deliver Uncompromised A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War*. [online] Mitre.org. Available at: https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-8AUG2018.pdf [Accessed 4 Sep. 2018].

[3] C. Nissen, J. Gronager, R. Metzger and H. Rishikof, "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War", *The MITRE Corporation*, 2018. [Online]. Available: https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security. [Accessed: 04- Sep- 2018].

[4] "Deliver Uncompromised: The Department of Defense's Latest Security Initiative | Accounting Services - Audit, Tax and Consulting | Aronson LLC", *Accounting Services - Audit, Tax and Consulting | Aronson LLC*, 2018. [Online]. Available: https://aronsonllc.com/deliver-uncompromised-the-department-of-defenses-latest-security/. [Accessed: 04- Sep- 2018].

[5] T. Temin, "Contractors hoping Congress can avoid shutdown despite DoD initiative", *FederalNewsRadio.com*, 2018. [Online]. Available: https://federalnewsradio.com/federal-drive/2018/08/2028606/. [Accessed: 04- Sep- 2018].