Securitization of Commercial Supply Chains: How Prescriptive Regulations of Defence Procurements Divide Industry and Government

Paul Hillier
Department of Political Studies
Queen's University, Kingston ON

EXECUTIVE SUMMARY

As commercial off-the-shelf products have become increasingly important to defence procurements, so too have the threats of infiltration to both government departments and private companies risen. This has motivated many countries to look at the role government can play in securing global commercial supply chains. In the United States, this happened in January 2011 when Congress gave the Department of Defense unprecedented powers to regulate commercial supply chains, namely the purview to blacklist contractors without oversight or transparency.

This policy brief argues that this new trend—the securitization of supply chains through prescriptive regulations—limits the federal government's ability to efficiently and effectively acquire mission critical technologies. This presents a credible national security risk, more grave than those the measures seek to mitigate. Although allowing industry to exclusively self-regulate the security of their products may not be a credible solution, it is recommended that the newly granted authority to regulate commercial supply chains must be rescinded.

CONTEXT AND IMPORTANCE OF THE PROBLEM

The Department of Defense (DoD) procures a substantial portion of its Information Technology (IT) from a small cadre of contractors, covering purchases as diverse as routers, software, or the components of fighter jets. To fulfil government needs, prime contractors utilise commercial off-the-shelf (COTS) products supplied by subcontractors. Given that prime contractors may know very little about employees

working for subcontractors—working in potentially any country in the world—the potential risk of infiltration and counterfeiting products grows exponentially with every link down the supply chain.

Supply Chain Risk Management (SCRM), originally developed by industry to proportionately manage the risks associated with subcontracting elements of the final product, began to be adopted by Western governments in the 1990s as public procurements became increasingly intertwined with global commercial supply chains (Peck, 2005; Peck, 2006; Erridge and McIlroy, 2002). The critical role that COTS play in American defense means that infiltration into the supply chain presents one of the most vulnerable periods of risk for the warfighter, and by every measurable standard, IT security breaches have risen over the past decade (Zhang and Suhong, 2006; Juttner, Peck and Christopher, 2003). The role of COTS in defence procurements has therefore grown in importance, while simultaneously having grown in vulnerability.

RECENT CHANGES IN POLICY

To deal with these risks, the newly passed H.R. 6523 National Defense Authorization Act for Fiscal Year 2011 contains a new strategy for SCRM located in Section 806 (S. 3454, 2010). This policy brief urges that Section 806 from H.R.6523 must be repealed due to the national security concerns presented by the delays it will cause to the procurement of mission critical technologies and the barriers of entry it will establish against smaller suppliers that hold many of these technologies.

At its core, Section 806 empowers the Director of the Defense Intelligence Agency and the Assistant Secretary of Defense for Networks and Information Integration to establish qualification requirements for the purpose of reducing supply chain risks by restricting procurement according to a number of guidelines.

> Sec. 806 (e)(2)(C): The decision to withhold consent for a contractor to subcontract with a particular source or to direct a contractor for a covered system to exclude a particular source from consideration for a subcontract under the contract (H.R. 6523, 2011).

However, the potential policy implications go far beyond guidelines and qualifications. In providing joint recommendations to agency heads, these offices play a key role in identifying sources or regions that need to be excluded from government procurement of covered items for national security purposes (H.R. 6523, 2011). This allows the federal government to disqualify a contractor on the grounds of a

perceived risk in its supply chain, effectively giving the DoD the purview to create a blacklist of contractors.

This blacklist may be based on geography—any supply chain that produces a mission critical component in a given at risk country may be blacklisted, a specific factory—any supply chain that produces a mission critical component in a factory suspected to be owned or operated by a foreign national army may be blacklisted, or even a specific employee—any supply chain that contains an employee suspected to be a counterintelligence operative may be blacklisted (H.R. 6523, 2011; ARWG, 2010). Many arguments against blacklisting have come from industry citing transparency as an integral value to cooperation in business; however, this policy brief maintains that encouraging DoD to wield such authority is an immediate national security concern.

CRITIQUE OF CURRENT POLICY OPTIONS

Section 806 leaves contractors no opportunity to sue in federal court or request disclosure through a Government Accountability Office (GAO) review to discover the source of the threat in order to rectify it (H.R. 6523, 2011)[1]. As such the primary opposition has come from contractors who maintain that blacklisting does not remove the security threat from the supply chain and, consequently, leaves potentially dangerous COTS to be procured by other federal government departments (ARWG, 2010). Primary support has come from the DoD, which lobbied the Senate and House Armed Services Committees (SASC & HASC) to include Section 806. DoD has argued that it requires this authority to effectively combat national security threats present in current supply chains, and maintains that blacklisting is not its primary intent, advising that it would only be used in the most extreme of circumstances (ARWG, 2010).

The primary roadblock to repealing this section is the weight that the HASC and SASC attach to arguments framed in terms of national security, particularly those made by the DoD. For this reason if industry concerns for regulation could be seen in national security terms, they would be strengthened and, thereby, able to compete with the threats that the DoD contends exist.

1 Section 806 came almost verbatim from Section 815 of S. 3454, the Senate-proposed National Defense Authorization Act for Fiscal Year 2011 that failed in December 2010 to even reach the Senate floor for a vote. Where this brief references lobbying for and against Section 806 of H.R. 6523, it is understood that much of the actual lobbying took place with reference to the almost identically worded Section 815 of S. 3454. A subsequent paper would be required to analyze the changes that were made to Section 815 in order to create Section 806.

Industry has charged that this section (and its predecessor, Section 815, S. 3454, 2010) is another example of a prescriptive regulation that prevents contractors from supplying cost-effective products in a timely manner and in a competitive and transparent environment (ARWG, 2010). COTS, which are the primary set of goods Section 806 regulates, are available through any commercial market and, as such, play a dominant role in global supply chains.

Regulations of COTS have traditionally been limited to internationally accepted Common Criteria, which industry is already meeting and self-enforcing. If we could speak of one unified industry perspective, it would be their demand that government leave them the freedom to decide how to go about fulfilling contracts (ARWG, 2010).

However Section 806 violates this by being prescriptive, telling industry how it must go about fulfilling contracts and, in so doing, granting a heretofore unparalleled power to the DoD: the power to blacklist a contractor with no transparency or oversight.

POLICY RECOMMENDATIONS

This policy brief emerges with two recommendations in light of industry's ultimately unsuccessful lobbying effort to prevent Section 806: (i) in order for Section 806 to be successfully repealed, it must be seen as yielding national security threats of its own; (ii) these national security threats caused by prescriptive regulations of the supply chain exist through two primary areas: first, by delaying the procurement of mission essential IT; and, second, by presenting barriers of entry to companies with critical technologies.

Risk management is defined, in a national security context, by weighing empirical threats according to the quantitative sum of two categories: the magnitude of the risk; and the probability of the risk materializing (Khan and Burnes, 2007; Knemeyer, Zinn and Eroglu, 2009). Therefore proving that the risk of infiltration to the supply is empirically lower than the risks presented by Section 806 itself would be methodologically unsound; too many variables associated with these types of risks are themselves not quantifiable in the ways that many academics have approached risk management (Ritchie and Brindley, 2007; Korosec, 2003; Khan and Burnes, 2007). Instead I charge that proponents of Section 806 are unable to show that the authority to blacklist a contractor is proportional to the threat. Furthermore, proponents cannot effectively defend against the claim that Section 806 has the

potential to cause more serious national security threats than it addresses. In so doing this brief shifts the debate towards seeing both arguments in a national security context. As such the remainder of this brief intends to show how delays and barriers of entry caused by Section 806 are also threats to national security.

The comparative advantage of technology that the DoD holds over potentially non-friendly state and non-state actors has decreased over that past decades, in large part due to the proliferation of COTS (Waters, 2007). Strategic advantages are rarely maintained by holding technologies that potential enemies do not, but instead by acquiring technologies before potential enemies can gain access to them.

COTS represent a growing array of technologies that actors may simply buy off the Internet, and increasingly include the most advanced technologies in their fields. Many DoD contracts fulfilled by the prime contractors utilise these same technologies in their supply chains (ARWG, 2010; Kennedy, 2000). When the United States regulates contractors' supply chains such as through Section 806, mandating changes to COTS, it becomes more efficient for non-friendly actors to procure these technologies before prime contractors may fulfil DoD contracts. Therefore recognizing delays as credible national security concerns shows that a transparent, rapid supply chain is a matter of national security and that overregulation in a prescriptive manner is itself an intrinsic threat.

The second contention this policy brief presents against Section 806 is that it creates barriers of entry that deter critical suppliers from the federal government market. Whereas the first argument explores delays, which affect procurement from all sizes of contractors, the barriers of entry created by Section 806 present a burden that is disproportionately shared by smaller contractors.

It is difficult to quantify the wariness many SMEs (small and medium-sized enterprises) hold towards the federal government as a customer, nor even to quantitatively show how many avoid the federal government market or for what reasons (Karjalainen and Kemppainen, 2008; Autry and Bobbitt, 2008). However despite the fact that many of these SMEs do not bid directly as prime contractors on DoD contracts, large companies utilise these technologies. Furthermore, these technologies are frequently integral components of larger procurements, necessitating their involvement in the procurement process.

Therefore, Section 806 is unique because it can prevent the prime contractors from using these SMEs even as subcontractors because of a single component or element DoD deems is potentially unsafe (H.R. 6523, 2011). SMEs are made even more critical due to the fact that in the defense market, there are rarely multiple sources in the area of critical technologies (Karjalainen and Kemppainen, 2008; Clark III and Moutray, 2004, Rose-Anderssen, Baldwin and Ridgway, 2011). As such, the DoD's failure to procure these mission critical technologies is a national security concern. Once a given supplier is blacklisted by Section 806, there is no reason to expect that DoD will be guaranteed to find a suitable replacement, especially when prime contractors are given no information to help them remove the threat. The threat is therefore not only left in the supply chain for other government agencies to procure, but DoD will be unable to procure technologies that non-friendly actors have the opportunity to buy from commercial markets (ARWG, 2010).

While barriers of entry disproportionately affect SMEs, large commercial companies—for whom the federal government is not necessarily their primary customer—may have strong motivations to exit the market. Stated simply, every commercial company has a tipping point when government regulations become overbearing and it is no longer in the company's interests to modify their COTS to sell in the federal government market. Between SMEs refraining from entering and the exiting of large commercial companies for whom the federal government is a small customer, it is evident that simple economic barriers deprive the federal government of technology that non-friendly actors may procure and allow them to garner a comparative technological advantage, thereby threatening national security.

CONCLUSION

Creating blacklists based on geography, ownership, or personnel compels prime contractors to change their supply chains from their commercial states, which profoundly increases prices of government procurements. However, defense offsets are just one example of many wherein government already demands changes to the supply chain (Rendon and Snider, 2010). What makes Section 806 unique—going beyond the immediate concerns for transparency and access to information—is that it introduces prescriptive regulations that are themselves national security threats.

This policy brief has contended that the way the debate has been framed, between national security on the one hand and economic costs on the other, will inevitably

fall in favour of national defence, especially as the primary constituents are the HASC and SASC. DoD maintains that the potential for infiltration into supply chains requires a proactive risk management plan, despite their inability to quantify the risks that will be created by barriers of entry and delays of mission essential procurement.

To conclude, there is a clear tension at play: commercial supply chains are growing increasingly critical to defence procurements while at the same time they grow increasingly vulnerable. The latter demands that some security measures are put in place and government must play a role in this; however, the former necessitates that excessive securitization of commercial supply chains will yield a negative impact. Ultimately, the inclusion of Section 806 should lead us to conclude that industry's lobbying proved less effective to that of the DoD, which demands that the issue be reframed to appreciate the national security threats on both sides of the issue. From there, while strictly self-regulation by industry may not be tenable, this brief has focused on arguing that Section 806 carries too many new threats to reasonably support.

WORKS CITED

Acquisition Reform Working Group (ARWG). "Comments on FY 2011 National Defense Authorization Act House-Passed H.R. 5136 and Senate Committee-Passed S. 3454." July 27, 2010. http://www.ndia.org/Advocacy/Resources/Pages/ARWG.aspx Accessed 20 Nov 2010.

Autry, Chad W and L Michelle Bobbitt. "Supply Chain Security Orientation: Conceptual Development and a Proposed Framework." *The International Journal of Logistics Management* 19.1 (2008): 42-64.

Clark III, M. and C. Moutray. "The Future of Small Businesses in the US Federal Government Marketplace." *Journal of Public Procurement* 4.3 (2004): 450–470.

The Common Criteria for Information Technology Security Evaluation. *Common Methodology for Information Technology Security Evaluation: Evaluation Methodology*. July 2009. http://www.commoncriteriaportal.org/ Accessed 15 Jan 2011.

Erridge, Andrew and John McIlroy. "Public Procurement and Supply Management Strategies". *Public Policy and Administration*, 17.1 (2002): 52-71.

Juttner, Uta, Helen Peck, And Martin Christopher. "Supply Chain Risk Management: Outlining an Agenda for Future Research." *International Journal of Logistics: Research and Applications* 6.4 (2003): 197-210.

Karjalainen, K., and K. Kemppainen. "The Involvement of Small- and Medium-Sized Enterprises in Public Procurement: Impact of Resource Perceptions, Electronic Systems and Enterprise Size," *Journal of Purchasing & Supply Management* 14 (2008): 230–240.

Kennedy, Harold. "Military Procurement Guide Being Revamped." *National Defense*, 85.560 (2000): 22.

Khan, Omera and Bernard Burnes. "Risk and Supply Chain Management: Creating a Research Agenda." *The International Journal of Logistics Management*, 18.2 (2007): 197-216.

Knemeyer, A. Michael, Walter Zinn, and Cuneyt Eroglu. "Proactive Planning for Catastrophic Events in Supply Chains. *Journal of Operations Management*, 27 (2009): 141-153.

Korosec, Ronnie Lacourse. "Assessing the Feasibility of Supply Chain Management within Purchasing and Procurement: Results from U.S. Cities." *Public Performance & Management Review*, 27.2 (2003): 92-109.

Peck, Helen. "Reconciling Supply Chain Vulnerability, Risk and Supply Chain Management." *International Journal of Logistics: Research and Applications*, 9.2 (2006): 127–142.

---. "Drivers of Supply Chain Vulnerability: an Integrated Framework. *International Journal of Physical Distribution & Logistics Management* 35.4 (2005): 210-232.

Rendon, Rene G. and Keith F. Snider. "Supply Management in American Public Administration: Towards an Academic Discipline?" *Journal of Purchasing & Supply Management*, 16 (2010): 99–108.

Ritchie, B. and C. Brindley. "An Emergent Framework for Supply Chain Risk Management and Performance Measurement." *Journal of the Operational Research Society*, 58.11 (2007): 1398-1411.

Rose-Anderssen, C, J.S. Baldwin, and K. Ridgway. "Commercial Aerospace Supply Chains: The Empirical Validation of an Evolutionary Classification Scheme." *Journal of Manufacturing Technology Management*, 22.1 (2011): 66-89.

United States. Cong. Senate. 111th Congress, 2nd Session. S 3454, *National Defense Authorization Act for Fiscal Year 2011*, (as introduced in the U.S. Senate; 4 Jun 2010). Library of Congress. Thomas. Web. 20 Nov 2010.

United States. Cong. 111th Congress, 2nd Session. HR 6523, Ike Skelton National Defense Authorization Act for Fiscal Year 2011, (Enrolled Bill [final as passed both House and Senate, 5 Jan 2011] – ENR) Library of Congress. Thomas. Web. 15 Jan 2011.

Waters, Donald. Supply Chain Risk Management: *Vulnerability and Resilience in Logistics*, London: Kogan Page Limited, 2007.

Zhang, Chen and Suhong Li. "Secure Information Sharing in Internet-Based Supply Chain Management Systems." *Journal of Computer Information Systems*, 46.4 (2006): 18-24.