Cyber Supply Chain Security and Potential Vulnerabilities within U.S. Government Networks

Megan Mance

June 15, 2016

Since 2008, the annual Worldwide Threat Assessment issued by the Director of National Intelligence (DNI) has listed cybersecurity as one of the greatest national security threats.[1] The current DNI, James Clapper told the Senate Select Committee on Intelligence in testimony on February 9, 2016 that cyber threats top the list once again saying, "innovation and increased reliance on information technology in the next few years on both our society's way of life in general and how we in the Intelligence Community specifically perform our mission will probably be far greater in scope and impact than ever."[2] On November 19, 2015 Admiral Michael Rogers the Chief of the National Security Agency and U.S. Cyber Command, told an audience that his principal concern is data manipulation through network intrusion.[3] U.S. adversaries are continually looking for new and creative ways to gain access to U.S. government networks. One specific cyber threat that deserves greater attention is cyber supply chain security within the federal government and the vital role of government contractors in this area.

The Department of Defense offers this definition for supply chain: The linked activities associated with providing materiel from a raw materiel stage to an end user as a finished product.[4] The U.S. government does not yet have a working definition of cyber supply chain security, however one research organization suggests it is, "the entire set of key actors involved with/using cyber infrastructure: system end-users, policy makers, acquisition specialists, system integrators, network providers, and software/hardware suppliers."[5] The number of stakeholders involved in cyber supply chain security highlights the need for an integrated approach to enhance security that involves close coordination between the private sector and the federal government.

[1] James R. Clapper, John D. Negroponte, Dennis C. Blair, and John M. McConnell, Worldwide Threat Assessment of the US Intelligence Community: Statement for the Record, Senate Select Committee on Intelligence, 2008-2016 but the date of this was not 2008-2016. When did this testimony occur?.

[2] Ibid.

[3] Cheryl Pellerin, "Rogers: Data Manipulation, Non-State Actor Intrusions are Coming Cyber Threats," DoD News, Defense Media Activity, November 19, 2015, http://www.defense.gov/News-Article-View/Article/630495/rogers-data-manipulation-non-state-actor-intrusions-are-coming-cyber-threats.

[4] United States, Department of Defense, Joint Education and Doctrine Division, J-7, DOD Dictionary of Military and Associated Terms, 2010, accessed April 4, 2016, http://www.dtic.mil/doctrine/dod_dictionary/.

[5] John Oltsik and Bill Lundell, ESG Research Report: Cyber Supply Chain Security Revisited, Publication, September 14, 2015, http://research.esg-global.com/reportaction/CyberSupplyChainRevisited/TOC.

The scope of government contracting and vulnerabilities introduced to government networks

To better understand the threat of such a large and complex cyber supply chain, it is important to consider the nature and extent of government contracting. In 2014, the federal government's prime contract obligations totaled around $447 billion[6] with over 2.3 million transactions.[7] While government contracting activity is not a new phenomenon and federal agencies have relied on the private sector to provide goods and services for decades, that reliance is becoming even more prevalent. As Information Technology (IT) solutions become more complex, agencies stand to save a lot of money by purchasing these services from the private sector or purchasing commercial off-the-shelf technologies rather than building their own systems.

In recent testimony to the House Committee on Oversight and Government Reform, federal Chief Information Officer Tony Scott commented, "Given the evolving threat landscape, it is imperative that we do everything in our power to ensure the security of government information and networks. In this interconnected world, we have to ensure that agencies, third-party contractors and vendors, and the citizens we serve all are protected from these threats."[8] This testimony was given just weeks before the Office of Personnel Management (OPM) announced two major network breaches compromising personally identifiable information of 21.1 million individuals, including current and former federal employees.[9] China was identified as the perpetrator and U.S. officials said their motive was to identify U.S. intelligence operatives and that stolen personal data about American citizens is part of a larger plan

[6] Annual Review of Government Contracting, 2015 Edition, Publication, National Contract Management Association and Bloomberg Government, 2015, accessed April 17, 2016, http://www.ncmahq.org/docs/default-source/default-document-library/pdfs/exec15---ncma-annual-review-of-government-contracting-2015-edition.

[7] Spending Map, 2016, accessed April 18, 2016, https://www.usaspending.gov/transparency/Pages/SpendingMap.aspx.

[8] *Testimony of Tony Scott United States Chief Information Officer, Office of Management and Budget Before the Committee on Oversight and Government Reform, United States House of Representatives, April 22, 2015*, 114th Cong, (2015) (testimony of Tony Scott).

[9] Ellen Nakashima, "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say," Federal Insider, July 9, 2015, accessed April 5, 2016, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

for China to increase intelligence collection.[10] What is noteworthy besides the scale of the information stolen is that this breach partly originated with a private contractor, KeyPoint Government Solutions, which conducted background checks for OPM. Hackers leveraged a compromised company credential to gain access to OPM's networks illustrating the risks confidential government systems can face in working with a vendor that has its own cybersecurity vulnerabilities.

Although federal leaders are aware of the need for enhanced security measures to protect networks and systems, there remain substantial flaws in the current system, and cyber vulnerabilities introduced by the global cyber supply chain add another layer of uncertainty. It should also be noted, that this is not a challenge unique to just the Department of Defense (DOD) or the Intelligence Community (IC); as demonstrated by the OPM breach, even agencies that do not handle national security issues directly have classified information on their networks that could be very dangerous in the wrong hands.

Complexities in the cyber supply chain have introduced new avenues for exploitation and manipulation attracting numerous U.S. adversaries

There exist a multitude of ways U.S. adversaries can insert themselves into the cyber supply chain. Private industry seems to be in agreement that the largest threats include: counterfeit parts, espionage through compromised devices, reverse engineering, intellectual property theft, and denial-of-service attacks.[11] According to estimates by the SANS Institute, up to 80% of all cyber breaches may have originated in the supply chain.[12]

In 2008, U.S. law enforcement seized over $75 million in counterfeit Cisco equipment including routers and switches that were already in use by the DOD, Federal Bureau of Investigation, and the Federal Aviation Administration.[13] In another example, China hacked into Lockheed Martin's networks

[10] Ibid.

[11] Davinic, Nick. *Booz Allen Hamilton- Vetting the Global Supply Chain.* Report. 2015. https://www.boozallen.com/content/dam/boozallen/documents/2015/06/Vetting-Global-Supply-Chain.pdf.

[12] Dave Shackleford, *SANS Institute White Paper: Combatting Cyber Risks in the Supply Chain,* Report, September 2015, https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252.

[13] John Oltsik and Bill Lundell, *ESG Research Report: Cyber Supply Chain Security Revisited,* Publication, September 14, 2015, http://research.esg-global.com/reportaction/CyberSupplyChainRevisited/TOC.

gaining access to millions of documents about the F-35 Joint Strike Fighter aircraft developed for the U.S. military.[14]

The government's largest contractors, which includes companies such as Lockheed Martin, Boeing, and Raytheon utilize a startling a number of suppliers when delivering mission critical systems and technologies to the U.S. government. Northrop Grumman alone revealed that in 2013, the company spent more than $8 billion dollars on approximately 9,500 suppliers.[15] Oftentimes, subcontractors and third party vendors do not have the same security controls in place as larger corporations, creating opportunities for hackers to gain access to networks or sensitive information. A recent article from SC Magazine wrote, "Many organizations do not possess reliable information about the vendors accessing their internal systems. According to a survey, just 35 percent of the decision-makers surveyed were 'very confident' that they knew how many vendors have access to their systems." [16]

Another concerning fact is that federal agencies have increased the number of set-aside awards for small to medium-sized companies. The Department of Homeland Security, for example, has set a goal for FY 2016 to award 33.5% of total contracts to small businesses.[17] The government contracting community has expressed concerns about the failure of small and mid-sized businesses to comply with common cybersecurity standards and as a result, these businesses represent some of the weakest links of the global supply chain.[18] A recent survey from the National Cyber Security Alliance shows that 59% of

[14] Fred Kaplan, "Who Gets to Define the Terms of Hacking?" The Atlantic, April 6, 2016, http://www.theatlantic.com/technology/archive/2016/04/who-gets-to-define-what-a-hacker-is/476838/.

[15] United States, National Institute of Standards and Technology, Department of Commerce, *Best Practices in Supply Chain Risk Management: Northrop Grumman Corporation Trusted, Innovative, World-Class Supply Chain,* By Kevin Engfer and Michael Ozmun, October 1, 2015, http://www.nist.gov/itl/csd/upload/NIST_USRP-Northup-Cyber-SCRM-Case-Study.pdf.

[16] Jeremy Seth Davis, "Reports Find High Security Risks among Policies for Third-party Vendors," *SC Magazine*, April 7, 2016, http://www.scmagazine.com/reports-find-high-security-risks-among-policies-for-third-party-vendors/article/488382/.

[17] "Small Business Goaling," The U.S. Small Business Administration, accessed April 6, 2016, https://www.sba.gov/contracting/contracting-officials/goaling.

[18] Statement of Thomas Michael Finan Chief Strategy Officer, ARK Network Security Before The U.S. House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies on "The Role of Cyber Insurance in Risk Management," 114th Cong., 9-10 (2016) (testimony of Thomas Finan).

small and medium businesses interviewed do not have a contingency plan in place for reporting and responding to data breaches.[19]

Research on this subject indicates there is a range of U.S. adversaries that would like to exploit vulnerabilities or manipulate the cyber supply chain. State-sponsored activities by China, especially as it relates to espionage and the loss of sensitive government information have been on the rise.[20] However, other adversaries such as terrorist organizations, other nation states, criminal enterprises focused on counterfeiting, and even insider threats need to be considered as potential threat actors.

Current government and private sector actions to mitigate threats have not gone far enough and additional actions are recommended to enhance cyber supply chain security

Government contractors, especially those belonging to the defense industrial base, have been very aware of the complexities and vulnerabilities of cyber supply chain security. They have crafted their own best practices as they relate to supply chain risk management, including sophisticated systems to oversee supplier performance, vetting processes for outside vendors, and strict adherence to ISO standards.[21]

As part of the FY 2012 National Defense Authorization Act additional authority was granted to the DOD, IC, and Department of Energy to exclude contractors from procurements for national security systems if they present a risk to the supply chain. This authority was reauthorized in subsequent years.[22] However, there are concerns among industry about ambiguities around the clause and the vague

[19] "New Survey Shows U.S. Small Business Owners Not Concerned About Cybersecurity; Majority Have No Policies or Contingency Plans," Staysafeonline.org (Powered by National Cyber Security Alliance), accessed May 5, 2016, https://staysafeonline.org/about-us/news/new-survey-shows-us-small-business-owners-not-concerned-about-cybersecurity.

[20] Molly Bernhart Walker, "Despite Pact, Clapper Remains Concerned about China's Cyber Espionage," *Fierce Government IT*, February 12, 2016, http://www.fiercegovernmentit.com/story/despite-pact-clapper-remains-concerned-about-chinas-cyber-espionage/2016-02-12.

[21] United States, National Institute of Standards and Technology, Department of Commerce, *Best Practices in Supply Chain Risk Management: Northrop Grumman Corporation Trusted, Innovative, World-Class Supply Chain,* By Kevin Engfer and Michael Ozmun, October 1, 2015, http://www.nist.gov/itl/csd/upload/NIST_USRP-Northup-Cyber-SCRM-Case-Study.pdf.

[22] Covington: DoD Issues Final Rule Addressing Exclusion of Contractors That Present Supply Chain Risk in National Security System Procurements, Publication, November 2, 2015, https://www.cov.com/~/media/files/corporate/publications/2015/11/dod_issues_final_rule_addressing_exclusion_of_contractors_that_present_supply_chain_risk.pdf.

formulation makes it difficult for defense contractors to fully grasp and execute their responsibilities in this effort insert additional security protection into the supply chain.[23]

While these efforts may be steps in the right direction for both contractors and government to take greater responsibility to protect their supply chains, much more needs to be done. Most concerning is the the average time it takes for an organization to detect a breach once its system is compromised. According to cybersecurity company FireEye the average time before an organization detects a breach on their network is 146 days.[24] That can mean the security of the supply chain is already compromised and finding where the breach originated could be incredibly difficult. By enhancing the cybersecurity posture of public and private organizations through network intrusion detection and continuous monitoring, the cyber supply chain will face less risk. Improving cyber defenses is much more of a challenge for small and medium-sized companies that are limited in their resources and capacity. If the government wants to do more business with these companies, it should devote resources to helping them achieve better cybersecurity and create incentive programs.

The President should designate a neutral standards organization, such as the National Institute of Standards and Technology (NIST) that is part of the Department of Commerce, to work with the private sector on developing a set of best practices around cyber supply chain security. NIST has been instrumental in helping developing cybersecurity best practices and guidelines to be adopted across the federal government and within the private sector. President Obama tasked NIST with developing a Cybersecurity Framework to enhance the security of critical infrastructure sectors in his Executive Order titled, "Improving Critical Infrastructure Cybersecurity."[25] As part of this effort NIST commented, "The framework, developed in collaboration with industry, provides guidance to an organization on managing

[23] Al Krachman/Blank Rome, LLP, "Ambiguities Cloud New Version of Cyber Defense Clause," *AFCEA Signal* (blog), April 6, 2016, http://www.afcea.org/content/?q=Blog-ambiguities-cloud-new-version-cyber-defense-clause.
[24] Derek Major, "Putting Cybersecurity Culture in the Spotlight," *Government Computer News*, April 13, 2016, https://gcn.com/articles/2016/04/13/security-culture.aspx.
[25] "Executive Order -- Improving Critical Infrastructure Cybersecurity," Executive Orders, February 12, 2013, accessed June 10, 2016, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

cybersecurity risk, in a manner similar to financial, safety, and operational risk." [26] NIST simultaneously created a companion publication called the *Roadmap for Improving Critical Infrastructure Cybersecurity*, which identified cyber supply chain security as an area that requires greater attention. [27] In October 2015, NIST held a workshop with some of the largest government contractors to have further dialogue on the topic of supply chain security and several publications were highlighted that emphasize best practices and organizational strategies to strengthen the security of the supply chain. [28] Additional resources should be devoted to NIST to continue their work in this area and their current findings need to be shared more broadly with the government contracting community.

While cybersecurity threats remain a focal point of current and recent Administrations, the vulnerabilities introduced by cyber supply chain security are not often part of the discussion. There also seems to be reticence by Congress to give serious consideration to the issue. In 2014, Representatives Ed Royce and Lynn Jenkins introduced the Cyber Supply Chain Management and Transparency Act, which would require government contractors to provide a list to procuring agencies of all open source and third-party components embedded in their software and also demonstrate these companies have no known cybersecurity issues. The bill was deferred to a Committee and never gained any traction after industry associations came forward expressing concerns that they do not agree with this approach for certifying vendors.[29] The tremendous complexities of the supply chain may be too intimidating and burdensome for government to take action on, especially in the current divisive state of Congress. Congressman Will Hurd who was a former CIA operative before being elected, acknowledged at a cybersecurity conference on April 12, 2016 that cyber supply chain security has been overlooked by the current Congress, but will become an increasingly important issue. He also said it begins with just simply educating policymakers

[26] Amber Corrin, "NIST Issues Preliminary Cybersecurity Draft Framework," FCW, August 28, 2013, accessed June 10, 2016, https://fcw.com/articles/2013/08/28/nist-cybersecurity-framework.aspx.

[27] "Best Practices in Cyber Supply Chain Security," National Institute of Standards and Technology, July 14, 2015, http://www.nist.gov/itl/csd/best-practices-in-cyber-supply-chain-risk-management-october-1-2-2015.cfm.

[28] "INDUSTRY BEST PRACTICES FOR CYBER SCRM," National Institute of Standards & Technology Computer Security Division, January 3, 2012, accessed July 16, 2016, http://csrc.nist.gov/scrm/industry_best_practices.html.

[29] Brian Heaton, "Will Open Source Security Be on the Federal Agenda in 2015?" *Government Technology*, January 8, 2015, http://www.govtech.com/security/Will-Open-Source-Security-Be-on-the-Federal-Agenda-in-2015.html.

on the topic to begin a dialogue. "Based on my time in the CIA and my understanding of our adversaries, this is a very serious threat," he commented.[30] While the private sector may fear greater regulation and compliance as this issue is more closely considered, it is within the country's national security interests to take greater action. Unfortunately, some cyber experts express deep concern that other breaches as serious as the OPM incident have already occurred on government networks and have yet to be discovered. The longer policymakers wait to consider how to enhance cyber supply chain security, the more vulnerable government networks become.

[30] Hurd, Will. "Government Keynote." Speech, FireEye Government Forum, DC, Washington, April 12, 2016.

Bibliography

Annual Review of Government Contracting, 2015 Edition. Publication. National Contract Management Association and Bloomberg Government. 2015. Accessed April 17, 2016. http://www.ncmahq.org/docs/default-source/default-document-library/pdfs/exec15---ncma-annual-review-of-government-contracting-2015-edition.

Bernhart Walker, Molly. "Despite Pact, Clapper Remains Concerned about China's Cyber Espionage." *Fierce Government IT*, February 12, 2016. http://www.fiercegovernmentit.com/story/despite-pact-clapper-remains-concerned-about-chinas-cyber-espionage/2016-02-12.

"Best Practices in Cyber Supply Chain Security." National Institute of Standards and Technology. July 14, 2015. http://www.nist.gov/itl/csd/best-practices-in-cyber-supply-chain-risk-management-october-1-2-2015.cfm.

Clapper, James R., John D. Negroponte, Dennis C. Blair, and John M. McConnell. *Worldwide Threat Assessment of the US Intelligence Community: Statement for the Record, Senate Select Committee on Intelligence*. 2008-2016.

Corrin, Amber. "NIST Issues Preliminary Cybersecurity Draft Framework." FCW. August 28, 2013. Accessed June 10, 2016. https://fcw.com/articles/2013/08/28/nist-cybersecurity-framework.aspx.

Covington: DoD Issues Final Rule Addressing Exclusion of Contractors That Present Supply Chain Risk in National Security System Procurements. Publication. November 2, 2015. https://www.cov.com/~/media/files/corporate/publications/2015/11/dod_issues_final_rule_addressing_exclusion_of_contractors_that_present_supply_chain_risk.pdf

Davinic, Nick. *Booz Allen Hamilton- Vetting the Global Supply Chain.* Report. 2015. https://www.boozallen.com/content/dam/boozallen/documents/2015/06/Vetting-Global-

Supply-Chain.pdf.

Davis, Jeremy Seth. "Reports Find High Security Risks among Policies for Third-party Vendors." *SC Magazine*, April 7, 2016. http://www.scmagazine.com/reports-find-high-security-risks-among-policies-for-third-party-vendors/article/488382/.

"Executive Order -- Improving Critical Infrastructure Cybersecurity." Executive Orders. February 12, 2013. Accessed June 10, 2016. https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

Heaton, Brian. "Will Open Source Security Be on the Federal Agenda in 2015?" *Government Technology*, January 8, 2015. http://www.govtech.com/security/Will-Open-Source-Security-Be-on-the-Federal-Agenda-in-2015.html.

Hurd, Will. "Government Keynote." Speech, FireEye Government Forum, DC, Washington, April 12, 2016.

"INDUSTRY BEST PRACTICES FOR CYBER SCRM." National Institute of Standards & Technology Computer Security Division. January 3, 2012. Accessed July 16, 2016. http://csrc.nist.gov/scrm/industry_best_practices.html.

Kaplan, Fred. "Who Gets to Define the Terms of Hacking?" The Atlantic. April 6, 2016. http://www.theatlantic.com/technology/archive/2016/04/who-gets-to-define-what-a-hacker-is/476838/.

Krachman/Blank Rome, LLP, Al. "Ambiguities Cloud New Version of Cyber Defense Clause." *AFCEA Signal* (blog), April 6, 2016. http://www.afcea.org/content/?q=Blog-ambiguities-cloud-new-version-cyber-defense-clause.

Major, Derek. "Putting Cybersecurity Culture in the Spotlight." *Government Computer News*, April 13, 2016. https://gcn.com/articles/2016/04/13/security-culture.aspx.

Nakashima, Ellen. "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say." Federal Insider. July 9, 2015. Accessed April 5, 2016. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

"New Survey Shows U.S. Small Business Owners Not Concerned About Cybersecurity; Majority Have No Policies or Contingency Plans." Staysafeonline.org (Powered by National Cyber Security Alliance). Accessed May 5, 2016. https://staysafeonline.org/about-us/news/new-survey-shows-us-small-business-owners-not-concerned-about-cybersecurity.

Oltsik, John, and Bill Lundell. *ESG Research Report: Cyber Supply Chain Security Revisited.* Publication. September 14, 2015. Accessed April 4, 2016. http://research.esg-global.com/reportaction/CyberSupplyChainRevisited/TOC.

Shackleford, Dave. *SANS Institute White Paper: Combatting Cyber Risks in the Supply Chain.* Report. September 2015. https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252.

"Small Business Goaling." The U.S. Small Business Administration. Accessed April 6, 2016. https://www.sba.gov/contracting/contracting-officials/goaling.

Spending Map. 2016. Accessed April 18, 2016. https://www.usaspending.gov/transparency/Pages/SpendingMap.aspx.

Statement of Thomas Michael Finan Chief Strategy Officer, ARK Network Security Before The U.S. House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies on "The Role of

Cyber Insurance in Risk Management", 114th Cong., 9-10 (2016) (testimony of Thomas Finan).

Testimony of Tony Scott United States Chief Information Officer, Office of Management and Budget Before the Committee on Oversight and Government Reform, United States House of Representatives, April 22, 2015, 114th Cong. (2015) (testimony of Tony Scott).

United States. Department of Defense. Joint Education and Doctrine Division, J-7. *DOD Dictionary of Military and Associated Terms*. 2010. Accessed April 4, 2016. http://www.dtic.mil/doctrine/dod_dictionary/.

United States. National Institute of Standards and Technology. Department of Commerce. *Best Practices in Supply Chain Risk Management: Northrop Grumman Corporation Trusted, Innovative, World-Class Supply Chain.* By Kevin Engfer and Michael Ozmun. October 1, 2015. http://www.nist.gov/itl/csd/upload/NIST_USRP-Northup-Cyber-SCRM-Case-Study.pdf.

United States of America. U.S. Department of Commerce. National Institute of Standards and Technology. *NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. By Jon Boyens, Celia Paulsen, Rama Moorthy, and Nadya Bartol. April 2015. http://dx.doi.org/10.6028/NIST.SP.800-161.