AU/ACSC/2016

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

CYBER SUPPLY CHAIN SECURITY

CAN THE BACKDOOR BE CLOSED WITH TRUSTED DESIGN, MANUFACTURING AND SUPPLY?

by

Stephen R. Van Etten, Maj, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Gregory F. Intoccia

Maxwell Air Force Base, Alabama

August 2016

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the U.S. government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

TABLE OF CONTENTS

FIGURES

Page

ABSTRACT

There are significant cybersecurity challenges confronting the Department of Defense (DoD) and other U.S. departments and agencies due to their reliance on globalized information technology (IT) marketplace with insufficient security measures in place for a cyber supply chain providing vital IT products destined for mission critical systems. An unsecured globalized cyber supply chain provides amply opportunity for malicious actors to compromise, corrupt, and introduce counterfeit cyber components destined for critical government systems designed to protect and defend U.S. national security. The literature describes a cyber marketplace and supply chain driven by costs, which has created numerous vulnerabilities. It also identifies U.S. directives, policies, and techniques that have done little in securing the cyber supply chain. This paper utilizes a problem/solution framework and focuses on some prevalent cyber supply chain security issues a globalized IT marketplace has with counterfeit parts, malicious state and non-state actors and that can potentially build in backdoors that threaten cybersecurity for all. Solutions to this complex problem will focus on mitigation efforts the DoD and other U.S. departments and agencies can take by adding required education and training, evaluating procurement decisions, enhancing testing procedures, and by building partnerships in order to work trust and integrity back in its cyber supply chain.

INTRODUCTION

Cyberspace is a domain that the United States relies on daily, full of growing security concerns. Electronic devices have proliferated worldwide, creating a dependence on computers and Internet connections. Cyberspace and the technology that enables it, has made the world more interconnected than at any other time in history. Although this has created significant advantages, it creates a very real vulnerability of users being targeted and subject to electronic attack. Both nation-states and non-state actors are exploiting any vulnerability that they can find, to steal, disrupt, threaten, compromise, or destroy information and services. These cyber attacks can come in many forms, but the most common ones are accomplished through the use of malware attacks using spyware, worms, Trojans and viruses. Other common attacks may come as a result of spear phishing[i] and denial-of-service attacks[ii].

There are many cyber vulnerabilities, but the most significant one for the United States is related to cyber technology's design, manufacturing, and supply chain process. The growing globalized information technology (IT) marketplace currently has very few, if any, security measures in place to protect against the counterfeiting, tampering or corrupting of microelectronic hardware, software, and firmware as they work their way through the cyber supply chain. This creates a significant problem for the United States and its national defense, given that the United States is dependent upon leading-edge microelectronic hardware, software, and firmware that are increasingly produced outside of the United States.[1]

One of the most serious concerns over cyber supply chain problems relate to "backdoors"

[i] Spear phishing- requests to obtain confidential information conducted over the Internet or through email under false pretenses to fraudulently obtain passwords or personal data.
[ii] Denial of Service attacks – attackers attempt to prevent legitimate users from accessing information or services, typically done by flooding a network with information.

being installed in microelectronic hardware or software during code development. With so much code necessary to write increasingly sophisticated and complex programs to accomplish an ever growing list of important economic and social tasks. Consequently, software can be readily modified with little or no notice, a problem that makes this cyber supply chain issues far more challenging than conventional supply chain problems faced by the U.S. with respect to physical products. In the cyber supply chain, backdoors can be inserted into software or IT system along with the addition of legitimate software during its development, through the use of viruses, worms, or other malware designed to insert a backdoor.[2] A study conducted by the International Data Corporation in 2013 found that "at least a third of all PC software is counterfeit."[3] Microelectronic hardware also faces similar threats, which can be even more challenging to identify and resolve once they are installed.

The more exposure cyber components have to an unsecured supply chain, the more exposed it is to tampering, and the more problematic it is to track for integrity, and trustworthiness. Counterfeit, corrupted, and compromised cyber components have already been located within Department of Defense (DoD) systems, planes, helicopters, and weapon systems due to this unsecured globalized cyber supply chain.

Many cyber components that go into U.S. systems designed to defend the United States against potential adversaries, who desire to target U.S. technology and systems, are produced and procured in adversary or competitor countries such as China. The DoD has acknowledged this growing threat by putting measures in place to increase supply chain risk management and establish trusted suppliers for certain cyber components going into DoD systems. Unfortunately, with the amount and type of technology layered into many of these cyber components, software, and firmware even with these processes in place it can be nearly impossible to tell whether a

cyber component has been compromised.

There are vulnerabilities associated with the increased globalization of the IT marketplace that present potential problems for the DoD and other U.S. government agencies. One vulnerability this marketplace presents is ease of access. This vulnerability enables enemy states, competitor states or non-state actors to compromise cyber IT that have potential to end up in DoD and other U.S. systems. First, many cyber components installed in U.S. systems designed to defend the U.S. against its competitors and adversaries who desire to target U.S. cyber systems are produced and procured in these countries. Second, scientists have shown that adversaries have the capability and are installing cyber backdoors in some of the worlds most secure, 'military grade' microchips.[4] With the globalized IT marketplace rapidly growing, and the increased reliance by the United States on the private sector to perform many security functions once thought to be only the province of the federal government, the potential for "backdoors" being built into cyber components, software, and firmware is a reality which puts DoD and other critical U.S. cyber systems at risk. Thirdly, once these modifications or backdoors have been built in, they can be nearly impossible to detect especially in the testing process. The miniaturization and complexity of microelectronic hardware, software and firmware has made it nearly impossible to detect whether a portion of the chip or software has been tampered with, built in, or compromised. The problems created by this globalized IT marketplace are significant and could potentially cause "exceptionally grave damage" to national security and cost the DoD an enormous amount of time and money to fix.

To address these concerns, this paper will explore the following question: "With the current globalization of an IT marketplace with few if any security measures built into its supply chain, what steps can the DoD take to mitigate the risk of compromised, corrupted, or counterfeit

hardware, firmware and software from being installed into DoD cyber systems?" This paper maintains that the DoD should establish a process that relies on trusted design, manufacturing, and supply for the majority of its cyber hardware, software and firmware to minimize exposure to the globalized IT marketplace and move closer to a more secure cyber supply chain. In other words, DoD should establish a process where cyber components destined for its systems, travels a trusted path established by first determining the integrity of the people and processes used to design, generate, manufacture, and distribute cyber hardware, software and firmware.[5]

This paper argues that employing a trusted design, manufacturing, and supply approach would give the DoD more oversight to address vulnerabilities, enhance security measures, and would address the design processes on a need-to-know basis while enhancing testing procedures to mitigate risk. Trusted design and trusted manufacturing also would mitigate the potential for counterfeit or corrupted cyber components from making it into DoD systems. The benefits of trusted design and manufacturing would likely cost more, but would confidently minimize DoD components from exposure to the unsecured globalized IT marketplace and keep production out of adversary or competitor countries who wish to compromise DoD systems. The DoD and other U.S. agencies reliance on trusted design and manufacturing would allow greater oversight, limit access, control production locations, minimize the potential for tampering, and increase accountability to deliver reliable cyber hardware, software, and firmware.

The framework for this research paper will utilize the problem/solution method. As background, the basics of cyber attacks will be introduced. Further, the impact of the globalization of the IT marketplace and many of the supply chain concerns will be discussed, including the fact that this phenomena has significantly lowered computing costs and has accelerated deployment of cyber technology. This will be followed by an overview U.S

government and DoD recognition of the problem and an introduction of the current Trusted Supplier program. Four criteria will be established as standards in assessing possible solutions: these will focus on cost, integrity, reliability, and traceability. An analysis of the counterfeit problem, dangers of products coming from China and the risk backdoors pose will then follow. The research paper will conclude with recommendations for potential solutions to the cyber supply chain problem.

BACKGROUND

Cyber Attacks

Cyber attacks are growing at an alarming rate around the world. The complexity and the ingenuity behind these attacks, changes on a daily basis. Countries, terrorist organizations, criminal organizations, organization insiders and individuals are all striving to strengthen their ability or acquire the ability to carry out cyber attacks. The current arms race occurring in the world is for cyber warfare capabilities. In comparison to land, sea, air, and space domains that require significant investment to operate within, the cyber domain requires much less investment to obtain similar effects. Attacks in the cyber domain are very unique compared to other domains. They can occur in milliseconds, typically from obscured sources, and can be initiated against integrated systems from a computer anywhere in the world without notice.[6]

There are several ways these attacks are commonly carried out in the cyber domain. The first is through direct input, typically accomplished via physical entry into a computer via a disc, memory stick, or through data entered on an attached keyboard.[7] Another method of attack occurs through computers connected directly to a network, which allows attackers access to other cyber systems on that network.[8] A third form of attack is accomplished through signal attacks, typically accomplished remotely over the Internet.[9] A fourth method of attack, often overlooked

involves the corruption of hardware, software, and firmware in the design or manufacturing process as these items go through the cyber supply chain.[10]

A few threats associated with this supply chain include: the insertion of counterfeit components or software, the addition of malicious logic to hardware or software, relying on untrusted, malicious or unqualified providers, and the introduction of hardware or software containing exploitable defects. This is something that has started to gain attention over the last decade within the DoD and other government agencies, but at this point there is no concrete plan to address the current supply chain risk.

Globalized IT Marketplace

Several decades ago governments, militaries, universities, and companies were typically the only ones that could afford or invest in electronics and computers. This started to change with the invention of the personal computer in the late 1970s and the creation of the World Wide Web around 1989. Since then, the pendulum started to swing and the electronics industry has shifted its focus more to the general consumer. The industry demand for consumer electronics is focused on high-volume production in a rapidly evolving market that has a short life cycle.[11] The increased demand over the last few decades and increased costs in production associated with each new generation of technology, has seen a technology industry once dominate in the United States shift overseas, primarily to Asia.[12] Companies have taken their business overseas since foreign countries provide labor at lower wages and many costs associated with production in these countries are less. Among the top thirteen microelectronic foundries in 2015, only one, GlobalFoundries is a U.S. based company, though even that company is foreign owned.[13]

One of the key reasons for the growing global IT marketplace has to do with the costs associated with building leading-edge microelectronics fabrication facilities, which can cost

companies several billions annually.[14] This cost, associated with the short life cycle of today's microelectronics industry, has seen U.S. companies' transitioning from being integrated device manufacturers (IDMs), and moving to a fabless company model that relies on pure-play foundries to fabricate its products. In 2015, eleven of the thirteen leading foundries were pure-play foundries, while only two were IDM's.[15]

This transition started in the late 1980s with the emergence of the foundry business model.[16] This model took off in the industry and separated the design and manufacturing process of producing microelectronics. This created fabless microelectronic companies, which allowed companies to focus their attention and resources on design, development and marketing of its microelectronic products. This formed and allowed pure-play foundries to focus on providing manufacturing solutions to fabless microelectronic companies for their products.[17] This in turn encouraged partnerships and alliances between IT companies and pure-play foundries that provided a competitive cost advantage for both companies. With this change companies have continued to move away from seeing a product from the beginning of research and development all the way through testing and packaging. Instead the actual fabrication of the product is being outsourced. This change is depicted in Figure 1 below.

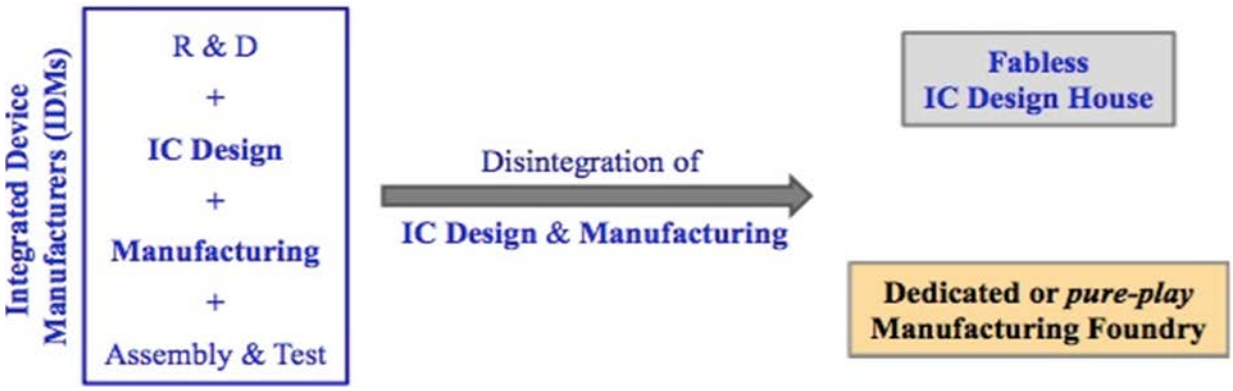

Figure 1. IDM shift to the fabless and foundry business model[18]

This trend in the marketplace has generated serious concerns for the DoD and other U.S. departments and agencies, which are heavily reliant on an industry that has gone global to meet their growing IT needs.[19] Now that most U.S. based companies are fabless or in the process of going fabless, this transition means a measure of security has been lost. This is something the DoD and other U.S. departments and agencies can not accept for microelectronic hardware, software and firmware destined for the most critical U.S. systems.[20] The challenge for the DoD is going to be its ability to influence a global arena for potential solutions to this security concern. This will be difficult because the DoD and other U.S. departments and agencies needs are significantly low in contrast to the general consumer market.

The other issue that this fast moving marketplace presents for the DoD is ready access to technologies that are older or have no commercial use. The life cycle for most microelectronics in the general consumer market is relatively short, driven by consumers who are looking for the newest and greatest technology. This means there is very little need to support older technologies, especially when factoring in the labor to fix older technology. It is typically cheaper and more advantageous to purchase the newer technology instead of paying to fix the old. This creates a problem for the DoD, whose needs are low–volume with unique requirements in comparison to the general consumer market. The additional problem this creates for the DoD, is that it generally needs support for long periods of time, with many weapon systems expected to be sustained over periods lasting decades.[21]

The growing globalized IT marketplace and continuing shift of technology development going overseas, has a strategic significance for the United States. This is due in part to the value the United States puts on IT and its ability to maintain a technological advantage within the DoD

and other U.S. departments and agencies.[22] For the United States and the DoD, it is critical that it develops a plan that will be supported, is actionable and will make sure the United States maintains its military superiority in the world.

United States Government and DoD Recognition of Cyber Supply Chain Risk

Supply chain risk is defined as: "The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."[23] The cyber supply chain security problem has been known for decades and initiatives have been under development for just as long, with the intent to secure it from the growing risks associated with the globalization of the IT marketplace. Despite such awareness and efforts, the supply chain threat has continued to grow. This major cyber threat is so significant that it now has the capability of affecting the development and operations of critical IT systems on whicht the DoD and other U.S. departments and agencies rely on.[24] The microelectronic hardware risk has been acknowledged as a serious problem for quite some time within the U.S. government; since the U.S. national defense and critical security systems are dependent on the microelectronics installed in these systems.[25] Since the early 2000s, there have been a number of initiatives to address the concern but none that have truly reduced the threat.

In 2002 the Federal Information Security Management Act (FISMA) was released requiring federal agencies to ensure their information technology systems incorporated appropriate information security safeguards.[26] The following year, in recognition of the DoD's reliance on leading edge microelectronics hardware and the increase in its production being sent overseas, the Deputy Secretary of Defense (DEPSECDEF) published the Defense Trusted IC

Strategy in 2003.[27] This established a series of initiatives that both the DoD and the National Security Agency (NSA) needed to move forward with to ensure that U.S. defense and security communities would have continued access to state of the art microelectronics required to meet the operational needs for mission critical and mission essential systems.[28] Figure 2 shows a history of trusted procurement policies since 2003.

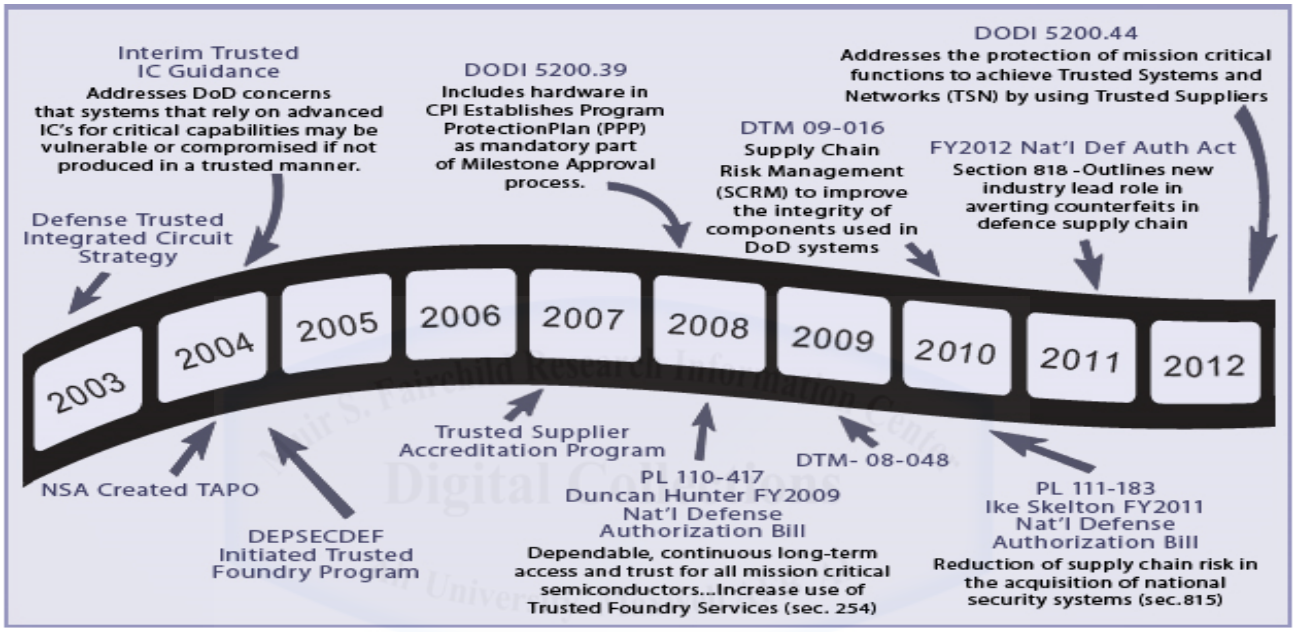

Figure 2. Trusted Procurement Policy History.[29]

In response to Defense Trusted IC Strategy the DoD and NSA created the Trusted Foundry Program with the goal of reducing the risk associated with a globalized IT marketplace relying on foreign manufactures. This program was designed to give the DoD and NSA the ability to track their microelectronics from end to end through a trusted domestic supply chain in a secure environment designed to ensure hardware assurance and integrity.

In 2004, the Bush administration issued Homeland Security Presidential Directive 12

(HSPD-12). HSPD-12 focused on individuals who worked in the cyber security supply chain. The goal was to identify individuals who might engage in fraud, tampering, counterfeiting and terrorist exploitation in order to gain access to the federal workforce and to critical infrastructure facilities.[30] In January of 2008, the Bush administration put together the Comprehensive National Cybersecurity Initiative (CNCI), which included National Security Presidential Directive 54 and Homeland Security Presidential Directive 24. These took at a multi-pronged approach to identify emerging cyber threats, looked to close gaps in current and future cyber vulnerabilities, and proactively respond to entities that desired to steal or manipulate secure federal systems.[31] In 2009 the Obama administration directed a Cybersecurity Policy Review that built on the CNCI. Within the CNCI was Initiative #11 which focused on developing a multi-pronged approach for global supply chain risk management.

The trend of cyber supply chain security concerns continues, as well as efforts to address them. In 2010, Section 806 of the 2011 National Defense Authorization Act (NDAA) authorized the DoD to consider the supply chain risk of a contractor, determine the risk that they may pose due to the lack of supply chain security, and if necessary exclude them from consideration.[32] By 2011 the Senate Armed Services Committee investigation of counterfeit electronic parts in military aircraft and weapons led to Section 818 of the 2012 NDAA which imposes many new supply chain obligations upon contractors of the DoD.[33] Also in 2012, the DoD issued instruction 5200.44, which looks to control the quality, configuration, and security software, firmware, hardware, and systems throughout their lifecycles.[34] In addition this instruction employs protections that manage risk in the supply chain for components or subcomponent products and services identifiable as having a DoD end-use.[35]

In 2013, the Obama administration issued a new Cybersecurity Executive Order (EO) in

response to the growing cyber threat to critical infrastructure. This Cybersecurity EO directed agencies to take specific actions to secure their critical infrastructure from physical and cyber threats.[36] One topic the Cybersecurity EO did not mention however, the growing problem associated with supply chain security risk, though it did acknowledge the need to include security standards in the acquisition planning and contract administration process.[37] It also called for detailed steps to harmonize and make consistent existing procurement requirements related to cyber security.[38]

From a cyber supply chain point of view, there seems to be wide recognition of a significant problem, evident by some of the initiatives, directives, acts or orders listed above. Yet, very little progress has been made in addressing and establishing actual solutions for the cyber supply chain security problems. Through all of this, efforts to defend against signal attacks seems to be the focus, while a compromised cyber supply chain delivering compromised hardware and software present an equally dangerous problem.[39] With this in mind, a Government Accountabilities Office (GAO) report found that the trusted supplier program is a primary risk reduction program for acquiring microelectronics for mission critical DoD systems.[40]

Existing DoD and NSA Trusted Foundry Program

The Trusted Foundry Program (TFP) was established in 2004 as a joint DoD and NSA program. This program was designed to ensure that both communities would have ready access to trusted leading-edge microelectronics for mission critical national defense systems provided by domestic sources.[41] This program started by partnering with IBM, a U.S. based company. IBM was able and willing to provide trusted leading-edge microelectronics through the design, fabrication, manufacturing, packaging and testing process.[42] This partnership worked well but a

single domestic supplier could not satisfy the entire DoD needs and the program was expanded to include other firms offering mature technologies that became the trusted supplier program managed by the Defense Microelectronics Activity (DMEA) within the DoD.[43]

In 2006, the DMEA was authorized to develop an accreditation process designed with the intent to engage other U.S. based microelectronic suppliers and bring them into the trusted supplier program.[44] As of April 2016 the program, according the DMEA website has 71 trusted suppliers including 22 with trusted fabrication process capabilities. Unfortunately, none of these suppliers provide the leading-edge capabilities of IBM that meet DoD needs, so the use of these suppliers has been minimal.[45] Unfortunately for the DoD, in July 2015, IBM's microelectronics fabrication business - the DoD's sole supplier of leading-edge technologies was transferred to GlobalFoundries, a U.S. based, but foreign owned entity.[46] In October 2015, a GAO report indicated there was uncertainty about whether the DoD would continue to have access to the trusted leading-edge technologies provided by IBM.[47]

Defense Microelectronics Activity (DMEA)

The DMEA was created to assist the U.S. Air Force with the emerging growth and necessity of microelectronics in weapon systems. The unit has evolved over the years under different agency heads. Today, DMEA reports to the Director for Defense Research and Engineering. It is an organization within the DoD with the unique mission of providing microelectronic components and assembly for DoD legacy systems. Legacy systems are older DoD systems that the current microelectronics industry cannot support with regular parts. DEMA provides long term support with a cradle to grave, total life cycle support management strategy.

DEMA works closely with companies through the Program Protection Plan process to

anticipate and make plans for parts obsolescence in mission critical systems.[48] This means participating suppliers must notify and give DEMA a two-year notice before they intend to stop production of any critical microelectronics.[49] The DEMA as mentioned above also manages the Trusted Supplier Program, which at this point in time is the most reliable and trusted way to mitigate risk when acquiring microelectronics for mission critical systems.[50] To become a trusted supplier the DEMA manages an accreditation program that mandates qualified suppliers follow a set of very stringent manufacturing and security obligations to receive and maintain an accreditation.[51] This program may be the best example of how the DoD can ensure microelectronics destined for mission critical systems are not exposed to tampering and will perform as intended when needed. Unfortunately, this program is too small in its current design to address the demand for new manufacturing needs of the DoD as a whole.

STANDARDS DoD SHOULD FOCUS ON IN CYBER SUPPPLY CHAIN

Cost

Cyber security remains an area of emphasis for the DoD and other U.S. departments and agencies this is clear with the funds dedicated to support it in recent budgets, but is it enough?

Government wide spending on Information Technology (IT) has seen a steady increase over the past 5 years from $75.4 billion in fiscal year (FY) 2011 to around $81.5 billion in FY 2016, right around an 8 percent increase.[52] The DoD's 38 percent share, $31 billion, is significantly higher than any other government agency.[53] This represents a decrease in IT spending decrease from around $35 billion in 2011 to $31 billion today.[54] With the reliance the DoD has on IT and the microelectronics that go into mission critical systems, the DoD needs to be increasing spending, not decreasing it in order to defend against sophisticated cyber attacks

that continue to grow.

The question is how does the DoD efficiently spend its money, encourage productivity, influence security measures, and maintain effective competition within its cyber supply chain? To properly spend its money DoD must establish strong relationships with the private sector and work closely with them to address these concerns. Efforts and funding should focus on better education, communication of requirements, expectations and clear guidelines for the procurement of IT and microelectronic components within the acquisition community. If the DoD and other U.S. departments and agencies do not shift more focus to securing the cyber supply chain they are going to likely spend more through the life cycle of IT and microelectronic components going into its systems. This cyber supply chain shift will likely result in higher acquisition costs up front, but should control and reduce costs for systems and products during their life cycle.

DoD IT spending is currently categorized into three areas; development, maintenance and service spending. For the DoD to improve and work towards a more secure cyber supply chain, DoD must put more focus in the area of development, which accounts for only 23 percent of the current IT spending, (see Figure 3).[55] Development Modernization Enhancement (DME) expenses are intended to; "substantively improve capability or performance, implement legislative or regulatory requirements; or meet an agency leadership request."[56] The capital costs that are included as a part of DME, "include hardware, software development and acquisition costs, commercial off –the-shelf acquisition costs, government labor costs for planning, development, acquisition, system integration, and direct project management and overhead support."[57] Figure 2 above outlines, the trusted procurement policies and initiatives in place since the early 2000s, but the DoD and other U.S. departments and agencies cyber supply chains

have not seen much positive change and have ultimately fallen short of meeting these policies. If the budget cannot be increased, funds should be shifted to DME from Operations and Maintenance (O&M) spending which accounts for 66.5 percent of IT spending in order to address these policies and focus on securing the cyber supply chain.[58] A secured and trusted cyber supply chain would likely see costs of O&M reduced with more reliable and trusted microelectronic hardware, software and firmware coming out of the cyber supply chain.

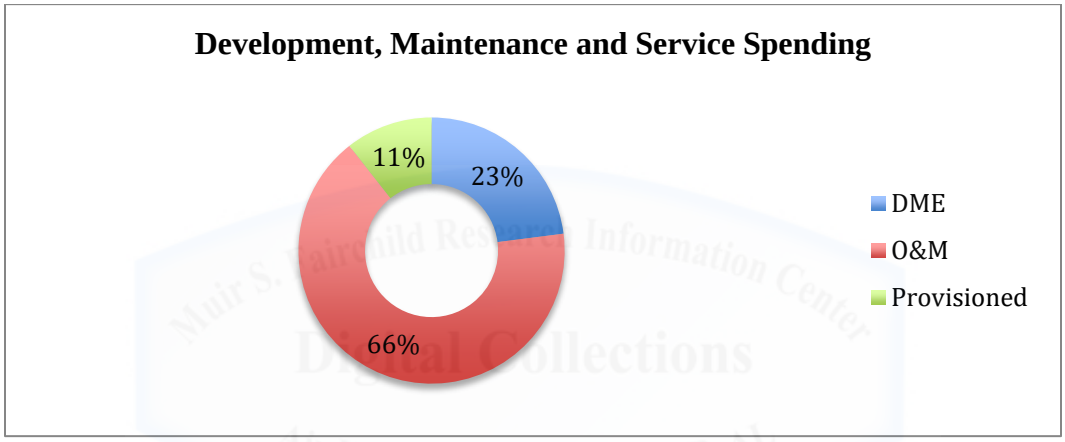

Figure 3. IT Development, Maintenance, and Service Spending[59]

While the globalization of the IT marketplace has added diversity, innovation, competition and lowered prices within the IT industry, it has seen a reduction in security. This has opened the opportunity for malicious actors to corrupt cyber supply chains by inserting counterfeit or malicious IT goods into the DoD and other U.S. departments and agencies cyber supply chains. Over the last decade a world economic crisis and budget cuts in the public and private sectors have resulted in budget cuts in manufacturing and security validation associated with the fabrication of IT products.[60] When talking costs, it is typically the determining factor

that influences the final choice for most buyers, especially government agencies who typically go with the low bid.[61] This is a bad practice to continue in the current globalized IT marketplace. If a product is priced significantly less than other competing products, this should bring up red flags, and questions should be asked before proceeding with the lower priced item such as: "How was it produced? Where is it from? Which software programming language was used to implement it? What vulnerabilities might I be accepting when I by the cheaper product?"[62] The DoD and other U.S. departments and agencies must change its mindset and rethink the low cost approach when it comes to products coming out of the globalized IT marketplace. The DoD and other U.S. departments and agencies must understand that a more secure cyber supply chain comes with increased costs and more funds must be allocated to improve assurances that microelectronic hardware, software and firmware being put into U.S. systems will be uncompromised and can be trusted.

Integrity

Integrity in IT is critical to the success of DoD systems and the mission critical weapon systems that rely on it. It is crucial that the microelectronic hardware, software and firmware come from the cyber supply chain have integrity. Currently, there is little integrity in the cyber supply chain and very few actionable measures have been taken by the DoD and other U.S. departments and agencies to make improvements. DoD should expect integrity from beginning to end in the acquisition process of its microelectronic hardware, software and firmware. This includes expecting a high degree of integrity from the people, systems, equipment and the logistical process that moves a product between them all.

One of the biggest and most challenging threats may be the insider threat, which is why holding personnel to high integrity standards and verifying that integrity is so important.

Integrity of personnel is important, there should be background checks and processes in place for continuous evaluation of personnel involved at all levels of the cyber supply chain. This process should be similar to the security clearance process and access control that the DoD and other U.S. departments and agencies use for access to information and facilities. There must be a well-established chain of custody that identifies personnel handling products from beginning to the end of the cyber supply chain process. Personnel throughout the cyber supply chain should only have access rights to critical information that applies to tasks needed to complete or accomplish their assigned duties. There needs to be integrity among DoD contractors and personnel working in the acquisition process and trust that they will follow policy, do their research, and use companies that have trusted processes in place. Ultimately, if personnel at all levels know they are being watched, held accountable and are held to a high level of integrity, a significant amount of risk will be mitigated. This reduces the likelihood of products being compromised as they move through the cyber supply chain.

Integrity does not end with the personnel involved in the cyber supply chain, it must also exist in the design, systems and equipment that create a product from research and development (R&D), to design, through fabrication, testing and packaging of a product. Security measures must be in place that makes the cost and time required to compromise products too high for an attacker. If the costs and effort needed are greater than the benefit to conduct an attack, malicious actors are less likely to carry out an attack. To do this security must be built into the product. Tests need to be built into the beginning and end of each process before it moves through the supply chain to make sure a product is clean and acting appropriately before additional layers are added. These processes and security measures should be revisited and evaluated to make sure holes are identified and those security gaps are closed. The DoD and other U.S. departments and

agencies must work closely with the private sector to promote and improve the integrity of the personnel, systems and processes that make up the cyber supply chain. Integrity built into these areas of the cyber supply chain will mitigate risk for DoD and other U.S. departments and agencies, while increase the trust of products coming out of it.

Reliability

Reliability is extremely important when it comes to the microelectronic hardware, software and firmware going into DoD and other U.S. departments and agencies U.S. cyber systems. If the IT purchased is unreliable, it can compromise missions, threaten national security, critical infrastructure and endanger the health and safety of personnel or bystanders. The DoD continues to invest in more technologically advanced IT systems and weaponry but if it is not reliable, the mission will fail. The DoD and other U.S. departments and agencies have a heavy reliance on advanced technology, reliability in this technology is key to them achieving national security objectives and a critical component to ensuring the U.S. military remains the most technologically advanced and superior fighting force in the world. Until, the DoD and other U.S. departments and agencies can establish in partnership with the public and private sectors a more secure cyber supply chain it must question and test everything coming out of it.

Traceability

Being able to trace parts is crucial to containing suspected or confirmed, compromised, corrupted, or counterfeit microelectronic hardware, software and firmware in DoD and other U.S. departments and agencies systems. There is no 100 percent guaranteed method to prevent attacks coming in through the DoD and other U.S. departments and agencies cyber supply chain. So in the event of an attack, when it is suspected or confirmed, compromised, corrupted, or counterfeit microelectronic hardware, software or firmware are identified as the cause, there

needs to be a quick way to locate and quarantine other similar items received from the same supplier. To accomplish this microelectronic hardware, software or firmware should have markings capable of being tracked in a database to quickly identify their location in order to remove them and eliminate future attacks or failures.

To track down and establish the origin of these compromised, corrupted, or counterfeit microelectronic hardware, software or firmware located in DoD and other U.S. departments and agencies systems products should have unique identifiers that allow track back through the cyber supply chain to potentially identify were the microelectronic hardware, software or firmware was compromised, corrupted, or counterfeited in the cyber supply chain process. Working with the supplier and keeping them informed of a potential security breaches would help them close potential security gaps in their cyber supply chain. This would also allow the DoD and other U.S. departments and agencies to reassess future use of these suppliers and report the breech for further investigation by law enforcement. Traceability in all areas of the cyber supply chain would be the ideal situation, but at a minimum there should be a way to track parts once they are installed or enter into DoD control.

ANALYSIS

Counterfeit Problem

The biggest problem produced by the globalized IT marketplace may be the large number of counterfeit IT products that continue to inundate the cyber supply chain. Defense Federal Acquisition Regulation Supplement (DFARS) defines counterfeit electronic parts as:

"…an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic

part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics."[63] These counterfeit parts do not discriminate and are finding their way into all levels of the cyber supply chain, those of private and public companies, the DoD and other U.S. departments and agencies. The more concerning part is that no one truly has a grasp on the impacts that these counterfeit parts have had the customers that have them installed in systems. Louis P. Feuchtbaum a former Naval officer and former attorney who represented large IT companies in dealing with counterfeit electronics and procurement fraud states the economic and safety issues involved with it are "indefinable and undeniable because they could be so grave."[64]

This counterfeit threat is a growing problem for not only the U.S. government but for U.S. business. This threat is costing millions of dollars a year in lost time, labor, and failing equipment. Over the past decade, there are a number of incidents where U.S. law enforcement has seized millions of dollars in counterfeit parts and or stopped the sale of them in sting operations. For example, federal authorities seized more than $143 million in counterfeit Cisco hardware and labels over a five-year period.[65] In 2008, a Saudi citizen attempted to sell counterfeit Cisco 100 gigabit interface converters bought in China to the DoD as genuine Cisco equipment.[66] Over a three-year period starting in 2007 U.S. authorities seized more than 5.6 million bogus semiconductors, with over 50 of these shipments falsely market as military or aerospace grade devises."[67] In 2011, "two people were convicted of selling as many as 59,000 counterfeit microelectronic circuits from China to the U.S. military, defense contractors, and others for use in U.S. warships, airplanes, missiles, and missile defense systems."[68] In 2012, the

FBI seized $76 million in counterfeit routers destined for U.S. government networks[69]. Then in 2014, an American contractor admitted to conspiring to traffic counterfeit semiconductors as new when they were actually refurbished and remarked to a U.S. Navy submarine base.[70] These are just a few of the many counterfeit seizures over the past few years. The bigger concern is how many of these shipments or sales are making it through the system and being installed into mission critical systems designed to protect and defend U.S. national security and creating a significant cyber security problem.

For the DoD, there have been a number of counterfeit parts that have made it through the cyber supply chain and been found in mission critical systems. A Senate report in 2012, "found 1,800 cases of counterfeit electronics parts involving over one million suspected parts," suspected of being in our cyber supply chain exposing some significant holes.[71] One of these cases identified 84,000 suspected counterfeit parts made it into the DoD supply chain from one supplier, where some of these parts made it into Traffic Alert Collision Avoidance Systems (TCAS) meant for installation in C5-AMP, C-12, and Global Hawk airframes.[72] Counterfeit parts have been located in Air Force aircraft made by Boeing, Lockheed Martin, and others to include the Missile Defense Agency (MDA) having 7 incidents of counterfeit parts be located in its own systems.[73] According to the MDA they also "found 800 fake parts on one missile interceptor system, at a cost of over $2 million dollars to replace them."[74] Figure 4 below shows a real versus counterfeit part located on a Navy P-8. There are too many of these reports and they, unfortunately, continue to grow. Even worse is there are significant amounts of counterfeit incidents that don't even get reported and even more cases that haven't even been identified. The DoD must start to build trust into its cyber supply chain and move quickly to mitigate the risk that counterfeit parts have on national defense, cyber security and more importantly the

danger they present to military personnel.

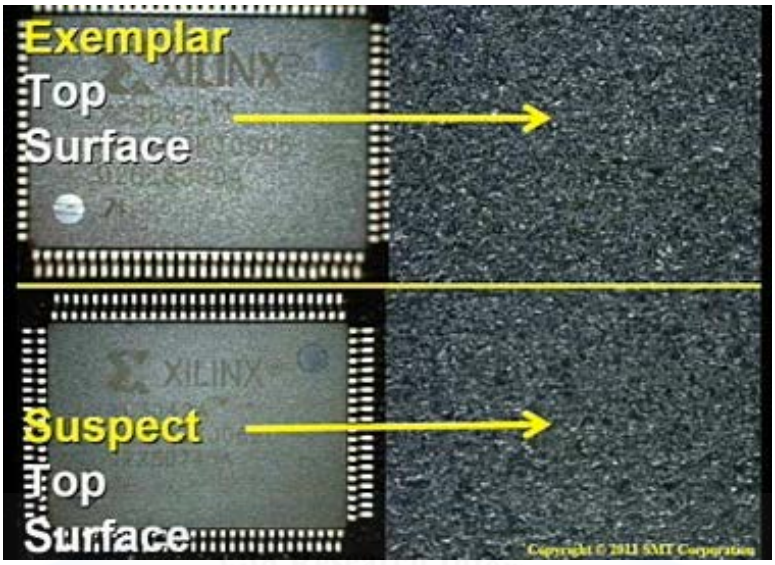

Figure 4. A sample of counterfeit parts located on Navy P-8. (http://www.electronics-lab.com/counterfeit-parts-found-on-p-8-posiedons/)

To resolve this problem, where does one start, the acquisitions process, the contractor, the supplier or the manufacturer considering there are problems at all levels. Section 818 of the fiscal year 2012 National Defense Authorization Act (FY 2012 NDAA) deals with the counterfeit issue tied to electronic parts and sets forth statues that require systems and procedures be put in place by large DoD contractors to detect and avoid counterfeit electronic parts. A recent proposed rule change by the DoD in late 2015 holds the same detect and avoid expectations and expanding the rule to small business, commercial and commercial off the shelf (COTS) suppliers. This is a great step in the right direction and should have occurred with its original release. In fact, there is a reason to believe the vulnerability of counterfeit parts is increased the further you go down the supply chain to smaller companies because they typically have fewer resources, procedures or capabilities to test, inspect and defend against counterfeits.[75] Regardless of the company size or

who the counterfeit product is supplied by, the risk it poses to the DoD and critical mission systems is the same. These rules are coming at the right time, but will only be effective if they are enforced.

One thing is clear counterfeits are a big concern as when it comes to cyber security, which threatens the reliability of computer networks and systems that the U.S. government relies heavily on. The other major concern is the risk of these inferior counterfeit parts being on mission critical weapon systems that the DoD depend on to protect and defend the United States. These counterfeits carry the capability of being corrupted with backdoors and are typically made of made of inferior products likely to fail. The vulnerabilities introduced by counterfeit parts could lead to mission failure and even worse could compromise the safety and lives of U.S. troops. The Government Accountability Office (GAO) did some investigating of the prevalence of counterfeit parts in DoD platforms. In one effort the GAO created a fictitious organization that purchased military-grade electronic parts and in one case, 7 of 13 parts they purchased and tested were suspected to be counterfeit.[76] That means nearly 54 percent of parts sold to the GAO as military-grade parts, were suspected of being counterfeit. These counterfeit parts coming in through the cyber supply chain present a clear threat to cyber and national security. Measures must be taken to identify and remove these counterfeits from the supply chain and eliminated the potential of hardware and software attacks that compromise cybersecurity, or the failure of these parts that could comprise the safety and lives of U.S. troops.

China

When looking at the major issues associated with the globalization of the IT marketplace that feeds the DoD and other U.S. departments and agencies cyber supply chain, a common theme that continues to be present in nearly every article, investigation or report, is China. The

People's Republic of China (PRC) is commonly a suspected source of cyber security threats and cyber supply chain risk.[77] There are many cybersecurity experts who have identified teams of hackers responsible for the theft of U.S. data; they have connected these attacks to the People's Liberation Army (PLA) of China and non-military groups sponsored by the Chinese government.[78] When looking at cyber supply chain risk, Chinese manufacturers account for one-fifth of the global IT marketplace and are also known to be a dominant source of supplying counterfeit electronic parts into the global cyber supply chain.[79] As a leader in cyber theft, manufacturing and as a leading source of counterfeit electronics in the cyber supply chain, China and the cyber products originating from their country are a threat to U.S. cybersecurity.

When looking at manufacturing, China is home to leading pure-play foundries producing microelectronic hardware, software, and firmware, which should draw concern for the DoD and other U.S. departments and agencies. This is concerning due to the control PRC has over companies within its borders and the influence they could or already have had in exploiting cyber vulnerabilities to further economic espionage or military exploitation.[80] Over the past decade millions of cyber attacks on U.S. entities, including the DoD have been traced back to China. There appears to be little doubt that China is stealing government and military secrets through hacking and by introducing corrupted and counterfeit electronic parts into the U.S. government cyber supply chain.[81] For this reason, U.S. intelligence officials believe IT products originating from China pose a significant threat to U.S. national security.[82] NSA has even intervened in purchases by U.S. companies and steered them away from purchasing from Chinese companies if they wanted "to continue its lucrative business with the U.S. government."[83] This is troubling, since a large amount of cyber components being produced in China are going into DoD mission critical systems. Especially, when China is actively making

strategic moves and building up its military with the intent to push the United States and its influence out of the Pacific.

Potentially, the most pressing concern with China is the large amount of counterfeit electronic parts that it floods into the cyber supply chain. China not only continues to be a leading source of counterfeit and pirated goods found entering the United States, they are also a leading source of counterfeit IT products.[84] An investigation by Senate Armed Services Committee determined "China is the dominant source for counterfeit electronic parts that are infiltrating the defense supply chain."[85] China is believed to account for close to 60 percent of the counterfeit electronics produced in the world[86] This statistic is not likely to change due to the rampant government corruption and little to no interest in stopping the counterfeiting, especially since they are sold openly in China's public market. "China continues to turn a blind eye to the rights of intellectual property (IP) holders and instead provides a host country to a billion-dollar black market industry for the creation of counterfeit electronics."[87] The Senate Armed Services Committee investigation also found that more than 70 percent of 100 suspected counterfeit parts located in the DoD supply chain were traced back to China. This percentage is troubling and the practice of acquiring microelectronic hardware and software for mission-critical systems coming out of China should be evaluated and heavily questioned.

Backdoors

Backdoors being built into microelectronic hardware and software destined for DoD and other U.S. departments and agencies systems are a major threat and risk that comes with a globalized IT marketplace and cyber supply chain. These backdoors can be introduced in a number of ways, introduced by malicious insiders during the design process, added during fabrication at a foundry, or built into counterfeit components being sold as the real thing to name

just a few. These backdoors can be designed to do a number of things, give an attacker control of a device, leak information, act as a gateway for access to other systems connected to the device, shut a device down or damage it permanently. Unlike traditional signal attacks, where the malicious actor must find a way into a system or device, with the backdoor, an attacker's path of attack is already built into the functionality of microelectronic hardware or software code before or during its fabrication. These typically remain dormant until triggered, which can launch a cyber attack designed to intercept classified intelligence, compromise critical infrastructure capabilities while undermining DoD ability to successfully complete its mission.[88] Building trust back into the U.S. government and DoD cyber supply chain would mitigate the risk of these backdoors being built in and adding another cyber security vulnerability to defend against.

When these backdoors or counterfeits are identified, the impact and fix can vary depending on whether the backdoor is built into the microelectronic hardware or software. If it is identified as a hardware attack, first you must locate and identify which piece of hardware is compromised or counterfeit, which can be very difficult due to a large number of hardware components most mission critical systems have. The second problem with compromised hardware is it cannot be altered or patched; it must be physically removed and replaced with a new hardware.[89] Then similar hardware devices must be located, tested and replaced in other systems containing the same device. Now when software is identified as having malicious code or of being counterfeit, the software can be updated, rewritten, or replaced. Hardware or software, the globalized cyber supply chain gives U.S. adversaries the ability to insert malicious backdoors that can have catastrophic effects capable of disabling or impairing critical DoD systems and weapons.[90] Currently, the capabilities for detecting these backdoors are limited and attackers seem to stay one step ahead in developing new evasion techniques, meaning current

capabilities can identify every kind of backdoor.[91] Preventing these backdoors is crucial and trusted design and manufacturing would drastically reduce the risk of them being maliciously installed in the design and manufacturing process where they are built in.

There are a number of suggestions to help protect against backdoors, they offer additional levels of security and monitoring but they also have the ability to present or create additional problems. With a potential of compromised chips slipping through the testing process, many articles on the topic suggest that there should be an additional level of security built into the microelectronic hardware. This can be accomplished by adding additional circuitry to the hardware designed to monitor the behavior of it and identify unusual activity indicative of an attack if attacked it would isolate any malicious activity, and notify other devices containing similar circuits.[92] Some other suggestions include a similar approach but have a self-destruct feature built into the hardware. These are great ideas in principle and having the defense built into hardware or software that doesn't require human intervention to stop an attack sounds intriguing. But, is adding more complexity to an already complex device or system is wise, this tends to add the potential for more exploitable flaws. There is potential that the additional circuitry could identify normal activity as an attack or falsely identify an attack and disable the system or device unnecessarily. In many cases, simplicity may be a better approach. While there are potential benefits to built-in hardware and software security, there may be just as many shortcomings that could cause effects similar to the attacks that the protection mechanisms are trying to prevent.

CONCLUSIONS

Clearly, the current globalized IT marketplace presents a significant threat with few if any security measures currently built into the current cyber supply chain. The threat of

counterfeits, countries like China and the potential of backdoors being built into cyber components has been acknowledged, but little been done to completely address it. The DoD and other U.S. departments and agencies must and can take steps to mitigate the risk of compromised, corrupted, or counterfeit hardware, firmware and software from being installed into mission critical cyber systems. By integrating trusted design, manufacturing, and supply practices while acquiring microelectronic hardware, software, and firmware, the overall risk to cybersecurity would be reduced. While there are a number of issues to address with the cyber supply chain, recommendations in this paper will focus on education, training, and accountability – enhance procurement and testing practices – and building partnerships to mitigate the risk associated with a globalized cyber supply chain and improve U.S. cyber security.

RECOMMENDATIONS

The benefits that the DoD and other U.S. departments and agencies reap with a globalized IT marketplace are at conflict with the security risks and unsecured cyber supply chain that it provides. While there may never be a 100 percent solution to securing the cyber supply chain, there are multiple approaches that must be taken to mitigate the risk associated with its globalization. Efforts must be taken to re-establish a level of trust and integrity in the cyber supply chain that is beneficial for the U.S. government and for those in the private and public sectors within its borders and those abroad. While there are a number areas that need to be addressed in regard to the globalized IT marketplace, there are a few things that will be helpful in mitigating the risk associated with the cyber supply chain. The DoD and other U.S. departments and agencies must start by focusing on internal practices and procedures before it starts to move out and resolve the cyber security issues created by the globalized cyber supply chain.

Education, Training, and Accountability

Without making or adding any additional policies, rules or initiatives designed to mitigate the security risks associated with the globalized IT marketplace, the DoD and other U.S. departments and agencies would see a rapid reduction in risk by doing a few simply things. It starts with educating, training and holding those affiliated with the procurement of microelectronic hardware, software and firmware accountable for following practices and rules already in place. There are sufficient risk management practices and resources in place, that if followed would reduce threats associated with the globalized supply chain but they must be practiced and implemented consistently at all levels to be successful.

For education and training, the DoD and other U.S. departments and agencies must have a clear understand of the threat posed by a globalized IT marketplace. There must be a concerted effort to educate personnel, contractors, and suppliers on the dangers present in a globalized cyber supply chain. There seems to be a lack of understanding in regard to the true threat faced by the DoD and other U.S. departments and agencies when looking at the cyber supply chain. The more education and heightened awareness at all levels will raise recognition of the risk, encourage more sharing of information and lead to enhanced practices designed to increase cyber security in the supply chain. Training must make people aware of the organizations, resources, and tools available to them and that they will be expected to utilize. These include things like the trusted supplier program and databases that list risky suppliers which people should check before ordering and procuring cyber parts. Increased education and training programs are a must for the DoD and other U.S. departments and agencies and would go a long way in raising awareness and increase the cybersecurity associated with U.S. procurement practices.

Enhanced Procurement and Testing Practices

Until the DoD and other U.S. departments and agencies feel there has been enough done to increase security and trust is built back in the cyber supply chain, purchases from high-risk suppliers and from fabrication facilities located in certain parts of the world should not be permitted. This means every effort should be made to eliminate the purchase of microelectronic hardware, software and firmware coming out of China or other countries that pose a similar cybersecurity risk. This will not be an easy task, but should be a requirement. Every effort should be made to make purchases from the original component manufacturer (OCM) and trusted suppliers of the OCM. Procurement from small business suppliers who are significantly removed from the OCM should be re-evaluated with the increased risk and potential they have of introducing corrupted, compromised or counterfeit parts into mission critical systems. The DoD and other U.S. departments and agencies must be willing to accept the additional costs that will likely be associated with this approach. While this may increase costs with the procurement of cyber components, decreasing the introduction of corrupted, compromised or counterfeit parts into the U.S. government should reduce the cost associated with cyber security and the life cycle costs tied to mission-critical systems.

Until the IT industry as a whole starts to address the security issues associated with the current cyber supply chain the DoD and other U.S. departments and agencies must work diligently to drastically improve its ability to test and validate microelectronic hardware and software being placed into its mission critical systems. Testing must move beyond simply testing that microelectronic hardware, software, and firmware is functioning as intended. While this is important, testing procedures and techniques must look for potential flaws or backdoors that may

have been introduced during the design or fabrication of a product. Forensic testing must be improved to identify and catch counterfeits coming through the cyber supply chain. This will help prevent them from being installed into DoD and other U.S. department and agency systems. While the DoD and other U.S. departments and agencies should expect suppliers and contractors to accomplish this, there are obvious holes and deficiencies in current testing procedures and practices from one supplier to the next. The DoD should invest in research and development teams who are focused on identifying corrupted, compromised or counterfeited microelectronic hardware, software and firmware coming through the global cyber supply chain. If the DoD wants to limit and mitigate the risk of these components from getting into its mission critical systems it needs to take more ownership and limit its reliance on suppliers and contractors to accomplish it for them.

Partnerships

The DoD and other U.S. departments and agencies will not be successful in moving towards a more secure cyber supply chain without working closely with the private and public sector to resolve the growing issue that threatens everyone and costs billions of dollars in damages ever year. The DoD and other U.S. departments and agencies must engage with U.S. IT companies and find ways to bring fabrication facilities back to the States. They must work closely with companies and suppliers to instill the value, importance and benefit a trusted cyber supply chain brings by establishing acceptable security practices that are financially beneficial for all. The U.S. government as a whole must work closely with allies and partners around the world and make a concentrated effort to change practices in the IT industry globally; the U.S. cannot do it alone. These partnerships must be viewed as beneficial for the global IT marketplace and the benefit of all who are a part of it, while it is critical to the cyber security of the U.S., they

must benefit everyone and not just the United States if real change is going to take place.

Notes

[1] Defined Business Solutions, LLC. "Cyber Defense Hardware Vulnerabilities." (April 12, 2011) 4.
[2] Michael I. Morrison, "The Acquisition Supply Chain and the Security of Government Information Technology Purchases." Public Contract Law Journal (March 12, 2013) 4.
[3] John F. Gantz et al., "The Dangerous World of Counterfeit and Pirated Software, International Date Corporation White Paper," (March 2013) 2.
[4] John Reed. "Proof That Military Chips From China Are Infected?" defensetech.org (30 May 2012).
[5] GAO. "Trusted Defense Microelectronics, Future Access and Capabilities Are Uncertain," GAO-16-185T (October 2015) 1.
[6] Defined Business Solutions, LLC. "Cyber Defense Hardware Vulnerabilities," 3.
[7] Ibid
[8] Ibid, 4.
[9] Ibid
[10] Ibid
[11] GAO. "Trusted Defense Microelectronics," 1.
[12] Ibid
[13] IC Insights. Major 2015 Foundries (Pure-Play and IDM), accessed 8/2/2016, http://www.icinsights.com/data/articles/documents/877.pdf
[14] GAO. "Trusted Defense Microelectronics," 1.
[15] IC Insights. Major 2015 Foundries (Pure-Play and IDM), accessed 8/2/2016, http://www.icinsights.com/data/articles/documents/877.pdf
[16] Samar K. Saha, "Emerging Business Trends in the Microelectronics Industry." Open Journal of Business and Management, 4, (2016) 106.
[17] Ibid
[18] Ibid
[19] Morrison. "The Acquisition Supply Chain," 5.
[20] J. Nicholas Hoover, "Secure the Cyber Supply Chain." Information Week. (November 9, 2009). 51.
[21] GAO. "Trusted Defense Microelectronics," 2.
[22] Ibid, 3.
[23] Ike Skelton National Defense Authorization Act for Fiscal 2011. Section 806. (Jan 7, 2011)
[24] Jarrellann Filsinger et al., "Chain Risk Management Awareness." Armed Forces Communication and Electronics Association Supply Cyber Committee, (February 2012) 9.
[25] Defined Business Solutions, LLC. "Cyber Defense Hardware Vulnerabilities," 4.
[26] Jeffery Chiow, Robert Metzger. "Cyber, Supply Chain and Information Security: New Developments & The Big Picture," Rogers Joseph O'Donnell. (February 2013) 4.
[27] Ibid
[28] Ibid
[29] Trusted Foundry, "Be Safe. Be Sure. Be Trusted." Accessed 7/23/2016. http://www.trustedfoundryprogram.org

[30] Morrison. “The Acquisition Supply Chain,” 15.
[31] John Rollins, Anna C. Henning, “Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations.” Congressional Research Service. (March 10, 2009) Summary.
[32] Chiow, Cyber, “Supply Chain and Information Security,” 2.
[33] Ibid
[34] DoD Instruction 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN).” (November 5, 2012)
[35] Ibid
[36] Chiow, “Cyber, Supply Chain and Information Security,” 5.
[37] Morrison. “The Acquisition Supply Chain,” 10.
[38] Ibid
[39] Defined Business Solutions, LLC. “Cyber Defense Hardware Vulnerabilities,” 5.
[40] GAO. Trusted Defense Microelectronics, 4.
[41] Defined Business Solutions, LLC. “Cyber Defense Hardware Vulnerabilities,” 5.
[42] GAO. Trusted Defense Microelectronics, 2.
[43] Defined Business Solutions, LLC.”Cyber Defense Hardware Vulnerabilities,” 5.
[44] GAO. “Trusted Defense Microelectronics,” 2.
[45] Ibid, 4.
[46] Ibid, 1.
[47] Ibid
[48] Chiow, Cyber, “Supply Chain and Information Security,” 3.
[49] Ibid
[50] GAO. “Trusted Defense Microelectronics,” 4.
[51] Ibid
[52] ITDashboard.gov, “IT Spending FY 2011-2017-Government wide.” accessed 8/3/2016, https://itdashboard.gov/
[53] Ibid
[54] Ibid
[55] ITDashboard.gov, “Development, Maintenance, and Services Spending,” accessed 8/3/2016, https://itdashboard.gov/
[56] Ibid
[57] Ibid
[58] Ibid
[59] Ibid
[60] Pierluigi Paganini, “Hardware Attacks, backdoors and electronic component qualification.” INFOSEC Institute. (October 13, 2013)
[61] Ibid
[62] Jarrellann Filsinger et al., “Chain Risk Management Awareness.” Armed Forces Communication and Electronics Association Supply Cyber Committee. (February 2012) 7.
[63] Defense Federal Acquisition Regulation Supplement and Procedures, Guidance, and Information. Subpart 2002.1-Definitions, Revised August 2, 2016.
[64] Michael B Kelly, “Counterfeit Chinese Microchips Are Getting So Good They Can’t Be Identified,” Business Insider. (June 16, 2012)
[65] Filsinger et al., “Chain Risk Management Awareness.” 2.
[66] Ibid

[67] Ibid
[68] Davis Inserra and Stephen P. Bucci Ph.D., "Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace," Backgrounder No. 2880, (March 6, 2014)
[69] David Goldman, "Fake tech gear has infiltrated the U.S. government," The Cybercrime Economy. (November 8, 2012)
[70] Don Sawyer, "Counterfeit threat taking malicious turn? Military Embedded Systems." October 6, 2014.
[71] Press release. "Senate Armed Services Committee Release Report on Counterfeit Electronic Parts," U.S. Senate Committee on Armed Services. (May 21, 2012) 1.
[72] Ibid, 2.
[73] Amber Corrin, "Counterfeit electronics in supply chain put contractors on the hook," The Business of Federal Technology, November 8, 2011.
[74] Ibid
[75] Ibid
[76] Corrin, "Counterfeit electronics in supply chain."
[77] Morrison. "The Acquisition Supply Chain," 6.
[78] Ibid
[79] Ibid
[80] Inserra, "Cyber Supply Chain Security," 6.
[81] Kelly, "Counterfeit Chinese Microchips."
[82] Morrison. "The Acquisition Supply Chain," 6.
[83] Ibid
[84] Goldman, "Fake tech gear."
[85] Press release. "Senate Armed Services Committee."
[86] Ibid
[87] John McHale, "Counterfeit IC threat evolves with spread of clone parts," Military Embedded Systems. (July 21, 2015)
[88] Sawyer, "Counterfeit threat taking malicious turn?"
[89] Inserra, "Cyber Supply Chain Security," 4.
[90] Ibid, 5.
[91] Paganini, "Hardware Attacks, backdoors," Detection.
[92] John D. Villasenor, "Ensuring Hardware Cybersecurity. Issues in Technology Innovation," Brookings. Issue 9. (May 2011)

BIBLIOGRAPHY

Chiow, Jeffery, Robert Metzger. *Cyber, Supply Chain and Information Security: New Developments & The Big Picture,* Rogers Joseph O'Donnell. February 2013.

Corrin, Amber. *Counterfeit electronics in supply chain put contractors on the hook,* The Business of Federal Technology, November 8, 2011. https://fcw.com/articles/2011/11/08/sasc-hearing-counterfeit-parts-dod-supply-chain.aspx

Defense Federal Acquisition Regulation Supplement and Procedures, Guidance, and Information. *Subpart 2002.1-Definitions,* Revised August 2, 2016.

Defined Business Solutions, LLC. *Cyber Defense Hardware Vulnerabilities,* April 12, 2011. www.definedbusiness.com

DoD Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN),* November 5, 2012.

Filsinger, Jarrellann, Barbara Fast, Daniel G. Wolf, James F.X. Payne and Mary Anderson. *Chain Risk Management Awareness.* Armed Forces Communication and Electronics Association Supply Cyber Committee, February 2012.

Gantz, John F., et al., *The Dangerous World of Counterfeit and Pirated Software,* International Date Corporation White Paper, March 2013. https://news.microsoft.com/download/presskits/antipiracy/docs/IDC030513.pdf

Goldman, David, *Fake tech gear has infiltrated the U.S. government,* The Cybercrime Economy, November 8, 2012. http://money.cnn.com/2012/11/08/technology/security/counterfeit-tech/index.html

Government Accountability Office, *Trusted Defense Microelectronics, Future Access and Capabilities Are Uncertain,* GAO-16-185T, October 2015.

Hoover, J. Nicholas, *Secure the Cyber Supply Chain*. Information Week, November 2009. http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=221600499

Ike Skelton National Defense Authorization Act for Fiscal 2011. Section 806, Jan 7, 2011.

ITDashboard.gov, *IT Spending FY 2011-2017-Government wide,* accessed 8/3/2016 https://itdashboard.gov/

Inserra, Davis, and, Stephen P. Bucci Ph.D. *Cyber Supply Chain Security: A Crucial Step*

Toward U.S. Security, Prosperity, and Freedom in Cyberspace. Backgrounder No. 2880, March 6, 2014. http://www.heritage.org/research/reports/2014/03/cyber-supply-chain-security-a-crucial-step-toward-us-security-prosperity-and-freedom-in-cyberspace

Kelly, Michael B., *Counterfeit Chinese Microchips Are Getting So Good They Can't Be Identified.* Business Insider, June 16, 2012. http://www.businessinsider.com/counterfeit-parts-from-china-raise-grave-concerns-for-both-us-companies-and-national-security-2012-6

McHale, John. *Counterfeit IC threat evolves with spread of clone parts,* Military Embedded Systems. July 21, 2015. http://mil-embedded.com/articles/counterfeit-threat-evolves-spread-clone-parts/

Morrison, Michael I. *The Acquisition Supply Chain and the Security of Government Information Technology Purchases.* Public Contract Law Journal, March 12, 2013.

Paganini, Pierluigi. *Hardware Attacks, backdoors and electronic component qualification.* INFOSEC Institute, October 13, 2013. accessed July 22, 2016. http://resources.infosecinstitute.com/hardware-attacks-backdoors-and-electronic-component-qualification/

Press release. *Senate Armed Services Committee Release Report on Counterfeit Electronic Parts,* U.S. Senate Committee on Armed Services, May 21, 2012.

Reed, John. *Proof That Military Chips From China Are Infected?*. Defense Tech. May 30, 2012. http://www.defensetech.org/2012/05/30/smoking-gun-proof-that-military-chips-from-china-are-infected/

Rollins, John and Anna C. Henning. *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations.* Congressional Research Service, March 10, 2009. https://www.whitehouse.gov/files/documents/cyber/Congressional%20Research%20Service%20%20CNCI%20%20Legal%20Authorities%20and%20Policy%20Considerations%20%28March%202009%29.pdf

Saha, Samar K. *Emerging Business Trends in the Microelectronics Industry.* Open Journal of Business and Management, (2016) 4, 105-113. http://dx.doi.org/10.4236/ojbm.2016.41012

Sawyer, Don. *Counterfeit threat taking malicious turn?* Military Embedded Systems. October 6, 2014. http://mil-embedded.com/articles/counterfeit-taking-malicious-turn/

Shockey, Jason R. *Combat readiness through Cyber Resilience.* Marine Corps Gazette. September 2015. https://www.mca-marines.org/gazette/2015/09/combat-readiness-through-cyber-resilience

Sternstein, Allya. *Forget Supersonic Jets. The Military Needs an Odometer for Computer Chips.*

Nextgov.com. September 26, 2014. http://www.nextgov.com/cybersecurity/2014/09/forget-supersonic-jets-military-needs-odometer-computer-chips/95246/

Villasenor, John D. *Ensuring Hardware Cybersecurity*. Issues in Technology Innovation, Issue 9. May 2011. http://www.brookings.edu/research/papers/2011/05/hardware-cybersecurity