NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CAN WE DEFEND THE DEFENSE SUPPLY CHAIN? LESSONS LEARNED FROM INDUSTRY LEADERS IN SUPPLY CHAIN MANAGEMENT

by

Ronald H. Menz

March 2018

Thesis Co-Advisors: Rodrigo Nieto-Gomez
Lauren Wollman

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 2018	3. REPORT TYPE AND DATES COVERED Master's thesis

4. TITLE AND SUBTITLE CAN WE DEFEND THE DEFENSE SUPPLY CHAIN? LESSONS LEARNED FROM INDUSTRY LEADERS IN SUPPLY CHAIN MANAGEMENT	5. FUNDING NUMBERS
6. AUTHOR(S) Ronald H. Menz	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

To protect the defense supply chain from counterfeit electronic parts, this thesis suggests that the Department of Defense (DOD) should adopt supply chain management methodologies used by Apple and the United Kingdom's Ministry of Defence (MoD). The paper explains how the 2011 Senate Armed Services Committee investigation exposed the problem of counterfeit components throughout the defense supply chain and describes the DOD's subsequent measures to address the issue, which have proven ineffective at best. The author uses two case studies and comparative analysis to identify and examine the practices Apple and the MoD use to protect their supply chains, some of which have become industry standards. The two case studies also highlight the disparities between the industry-recognized best practices in supply chain management and current DOD practices. Based on analysis of the case studies, the thesis provides a number of policy recommendations that the DOD could employ as part of its strategic effort to improve and protect the defense supply chain from counterfeit components.

14. SUBJECT TERMS counterfeit, components, supply chain management	15. NUMBER OF PAGES 105
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

CAN WE DEFEND THE DEFENSE SUPPLY CHAIN? LESSONS LEARNED FROM INDUSTRY LEADERS IN SUPPLY CHAIN MANAGEMENT

Ronald H. Menz
Supervisory Customs and Border Protection Officer (Port Director),
U.S. Customs and Border Protection Office of Field Operations
B.S., Hilbert College, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2018

Approved by: Rodrigo Nieto-Gomez
Thesis Co-Advisor

Lauren Wollman
Thesis Co-Advisor

Erik Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

To protect the defense supply chain from counterfeit electronic parts, this thesis suggests that the Department of Defense (DOD) should adopt supply chain management methodologies used by Apple and the United Kingdom's Ministry of Defence (MoD). The paper explains how the 2011 Senate Armed Services Committee investigation exposed the problem of counterfeit components throughout the defense supply chain and describes the DOD's subsequent measures to address the issue, which have proven ineffective at best. The author uses two case studies and comparative analysis to identify and examine the practices Apple and the MoD use to protect their supply chains, some of which have become industry standards. The two case studies also highlight the disparities between the industry-recognized best practices in supply chain management and current DOD practices. Based on analysis of the case studies, the thesis provides a number of policy recommendations that the DOD could employ as part of its strategic effort to improve and protect the defense supply chain from counterfeit components.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
- **A. RESEARCH QUESTION 1**
- **B. PROBLEM STATEMENT 1**
- **C. RESEARCH DESIGN 4**
- **D. LITERATURE REVIEW 5**
  - **1. The Defense Supply Chain 5**
  - **2. Counterfeits and the Defense Supply Chain 6**
  - **3. Apple and the United Kingdom's Ministry of Defence: Industry Leaders in Supply Chain Management 10**

II. DEPARTMENT OF DEFENSE PROCUREMENT BACKGROUND 13
- **A. DEPARTMENT OF DEFENSE PROCUREMENT 13**
- **B. IDENTIFICATION OF COUNTERFEITS IN THE DEFENSE SUPPLY CHAIN 14**
- **C. THE RESPONSE TO COUNTERFEITS IN THE DEFENSE SUPPLY CHAIN 18**
  - **1. Section 818 ..... 19**
  - **2. Final Rule 21**
  - **3. Review of Reporting Process 22**
  - **4. Industry Concerns 23**

III. APPLE: *THE* INDUSTRY LEADER IN SUPPLY CHAIN MANAGEMENT 25
- **A. APPLE'S ORIGINS 25**
- **B. NEW PRODUCT DEVELOPMENT 27**
- **C. PROCUREMENT 30**
- **D. PRODUCT ASSEMBLY 33**
- **E. LOGISTICS 35**
- **F. CONCLUSION 37**

IV. UNITED KINGDOM MINISTRY OF DEFENCE 39
- **A. OVERVIEW 39**
- **B. PROCUREMENT 41**
- **C. POLICY GUIDANCE 44**
- **D. COLLABORATIVE APPROACH 45**
- **E. CONCLUSION 47**

V. FINDINGS AND CONCLUSIONS 49
A. FINDINGS 50
1. Integrated Approach to Supply Chain Management 50
2. Collaboration 51
3. Contracting Practices 52
4. Policy 53
B. RECOMMENDATIONS 54
C. AREAS FOR FUTURE RESEARCH 55

APPENDIX. GT ADVANCED TECHNOLOGIES CHAPTER 11 BANKRUPTCY FILING 59

LIST OF REFERENCES 83

INITIAL DISTRIBUTION LIST 87

LIST OF FIGURES

Figure 1. Counterfeit Integrated Circuit 16

Figure 2. MoD Contracting for Availability: Partnering with Industry 43

Figure 3. Cost per Flying Hour for Tornado and Harrier Aircraft 43

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADI	Analog Devices Incorporated
CBP	Customs and Border Protection
CEO	chief executive officer
DOD	Department of Defense
FBI	Federal Bureau of Investigation
GAO	Government Accountability Office
IEEE	Institute of Electrical Electronics Engineers
MoD	Ministry of Defence (United Kingdom)
OECD	Organization for Economic Cooperation and Development
R&D	Research and Development

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Nearly six years ago the Senate Armed Services Committee investigation exposed how inundated the defense supply chain had become with counterfeit electronic components. The investigation identified vulnerabilities throughout the supply chain and highlighted counterfeit components found in missile systems, aircraft, and other sensitive technologies. These revelations sent shock waves through the defense industry and military community. In response to the Senate Armed Services Committee investigation, other countries began to ask whether their defense supply chains had been compromised by counterfeit electronic components, thus putting their national security at risk.

The immediate response was a bipartisan amendment to the 2012 National Defense Authorization Act. Congress' action was meant to strengthen the defense supply chain by implementing counterfeit avoidance protocols across the entire defense industry. However, this intent was not realized. While Congress' initial action was almost instantaneous, its actual implementation did not occur until 2014, two years later, when the final rule was issued. Compounding the measure's unrealized impact was the lack of guidance given to industry. As part of the final rule, defense contractors were to have measures in place for detecting and defending against counterfeit components. However, neither the amendment nor the final rule provided the guidance that industry wanted, and needed, to ensure all parties were doing their part to fight counterfeit components.

This thesis seeks to identify how the defense supply chain can defend against counterfeit electronic components by identifying and applying the best practices of industry leaders in supply chain management. To achieve this, the author used a comparative case study methodology to assess how two different organizations prevent counterfeit components from entering their supply chains. The two model entities selected for this analysis were Apple and the United Kingdom Ministry of Defence (MoD).

In researching the methodologies that Apple and the MoD use to manage their respective supply chains, this thesis identified a number of key concepts. Many of these

practices are now identified as the industry standard. Accordingly, a broad spectrum of industries use these methodologies to manage their supply chains, and they have helped establish a set of best practices for supply chain management. Based on these findings, the author makes the following recommendations to help the Department of Defense (DOD) apply these concepts to the defense supply chain.

- **Integrated Supply Chain:** The defense supply chain needs to adopt a singular approach to supply chain management. In this philosophy, supply chain management starts with product development and is interwoven through every other aspect of the procurement cycle, to include manufacturing, procurement, and logistics.

- **Collaborative Efforts:** The DOD needs to work more collaboratively with its industry partners. This includes providing industry with the needed guidance for implementing and measuring a counterfeit components detection model, as required in section 818 of the National Defense Authorization Act of 2012.

- **Contracting Practices:** The DOD needs to adopt a contracting for availability model similar to the UK MoD's model. In so doing, it must reapportion the level of responsibility assumed by defense contractors, which will afford the DOD greater leverage in its contracting practices.

- **Policy:** The DOD needs to more effectively develop and use policy to guide the actions of defense contractors and suppliers. While it has issued internal guidance to address the detection and prevention of counterfeit components, it has yet to provide industry with any such guidance.

ACKNOWLEDGMENTS

I am grateful to CBP Director of Field Operations Rose Brophy and Assistant Director of Field Operations Mike Millich for nominating me to attend the CHDS master's program. I also want to thank Area Port Director Cary Frieling and Assistant Area Port Directors Mark MacVittie and Joseph Zawistowski, who allowed me the time away for the in-residence sessions, and all the other days I needed to complete my thesis. Their support was instrumental to my successful completion of the program, and for that I am truly appreciative.

I want to thank the CHDS faculty and staff for the unending commitment and support they provide to every student. It is easy to see that, for many of them, this is truly a passion. Accordingly, I need to recognize Greta Marlatt. Greta's knowledge and talent are only surpassed by the level of care she demonstrates for each student, through her unstinting efforts to help each one through the academic process. Thank you, Greta, for everything you do; it is sincerely appreciated. Thank you to Dr. Rodrigo Nieto-Gomez, my patient and tolerant thesis co-advisor. His insightfulness and discerning use of the Socratic method continually served as the impetus to move my thesis forward and ultimately across the finish line. Thank you to Dr. Lauren Wollman, my empathetic but demanding thesis co-advisor. Her blunt yet caring tell-it-like-it-is style always served to get me beyond the seemingly insurmountable obstacles.

I also need to thank my colleagues and friends from cohorts 1603/1604. At the start of this journey, the focus was on the academic process. However, very early in the program it became much more than an academic endeavor. As our friend and brother Keith McKinney would say, "Life is about the experiences." So, whether it was touring the White House, sharing a class meal cooked by "Sweet G," spending all day locked in the thesis lab, or hoisting a glass in salute at the end of the day, there are innumerable experiences that I will forever remember. For this, I am truly grateful to all my classmates and friends.

Finally, and most importantly, I want to thank my family, starting with my girls, Sara, Shannon, Sidney, and Shaeleigh. Thank you for your understanding when Daddy couldn't be at your swim meets, Science Olympiad, and even a vacation during these eighteen months. My hope is that you will come to know I did this with you always in my mind. To my wife, Laura, who supported me not only for the last eighteen months but during every career and educational opportunity over the last twenty years: Throughout each of these endeavors you selflessly endured my abences, the demands on my time, and my moments of doubt. It is because of your endless love and support that I was able to do this and everything else we have accomplished. With all my love, I am forever grateful.

I. INTRODUCTION

A. RESEARCH QUESTION

This thesis answers the question, how can we defend the defense supply chain against counterfeit electronics?

B. PROBLEM STATEMENT

As our defense systems' and warfighters' capabilities continue to advance, so does their reliance on technology; many of these defense systems and their equipment contain mission-critical electronic components. The presence of counterfeit electronic components in the defense supply chain has been highlighted through different enforcement efforts and congressional investigations, the most significant of which was completed in 2011 by the Senate Armed Services Committee.[1] For the purpose of the Senate Armed Services Committee investigation, a counterfeit electronic part may include "both fakes and previously used parts that are made to look new and are sold as new."[2] The Committee determined "that vulnerabilities throughout the defense supply chain allow counterfeit electronic parts to infiltrate critical U.S. Military Systems, risking our security and the lives of the men and women who protect it."[3] The investigation also found that 70 percent of counterfeits come from China and that a significant percentage of the remaining counterfeits can be traced back through the supply chain to China.[4]

Of the many examples cited in the Senate Armed Services Committee report, the counterfeit electronic parts in the Navy's P-8A Poseidon aircraft bear the potential for generating the greatest number of fatalities. The P-8A is a modified Boeing 737 operated by a crew of nine that carries a payload of torpedoes and cruise missiles to support its

---

[1] *The Committee's Investigation into Counterfeit Electronic Parts in the Department of Defense Supply Chain*: *Hearing before the Committee on Armed Services United States Senate*, 112th Cong (2011).

[2] Ibid., 2.

[3] "Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts," U.S. Senate Committee on Armed Services, accessed December 13, 2017, https://www.armed-services.senate.gov/imo/media/doc/SASC-Counterfeit-Electronics-Report-05-21-12.pdf.

[4] Ibid.

anti-submarine and anti-surface warfare capabilities.[5] Following the U.S. Navy's acquisition of the aircraft, the manufacturer, BAE Systems, discovered defective parts. The components, which BAE Systems believed to be new, turned out to be used parts that had been resurfaced and remarked, and were ultimately traced back to a supplier in China.[6] If a Poseidon aircraft were to crash as a result of the counterfeit components, there is the likelihood of significant additional losses beyond the probable nine crewmember fatalities, especially if the incident occurred in a residential area similar to the 2012 F-18 crash in Virginia Beach.

This problem is not limited to the defense supply chain. In a report titled *The Economic Impacts of Counterfeiting and Piracy*, the International Chamber of Commerce estimated that total trade for counterfeited and pirated goods in 2013 was $461 billion.[7] Some of the factors driving this issue include the increasing complexity of supply chains due to globalization and the loss of data resulting from outsourcing and the ultimate need for cheaper and faster development.[8] The emergence of Asian electronics firms as market leaders has exacerbated the issue, as fake parts tend to be produced in close proximity to legitimate industries.[9] There have even been occurrences of counterfeiting in legitimate factories, allowing counterfeiters to feed off of the same supply chain.[10]

In spite of these factors, and in contrast to the defense supply chain, some industry leaders have bolstered proven track records of superior supply chain management. Of these, the clear leader is Apple. Apple has been ranked number one in supply chain

---

[5] "Aircraft and Weapon: P-8A Poseidon," Naval Air Systems Command, October 7, 2017, http://www.navair.navy.mil/index.cfm?fuseaction=home.display&key=cfd01141-cd4e-4db8-a6b2-7e8fbfb31b86.

[6] Ibid.

[7] Frontier Economics, "The Economic Impacts of Counterfeiting and Piracy" (report, International Chamber of Commerce, 2016), https://cdn.iccwbo.org/content/uploads/sites/3/2017/02/ICC-BASCAP-Frontier-report-2016.pdf.

[8] Eric Savitz, "Managing the Risks of a Globalized Supply Chain," *Forbes*, October 4, 2012, https://www.forbes.com/sites/ciocentral/2012/10/04/managing-the-risks-of-a-globalized-supply-chain/#5e71b21539d8.

[9] Ned Levin, "China's Counterfeits in the Spotlight," *Financial Times*, November 26, 2013, https://www.ft.com/content/8ab95c8e-4c7c-11e3-923d-00144feabdc0.

[10] Ibid.

management by Gartner Research since 2011, and achieved "Masters" status in 2015.[11] This rise to industry leader in supply chain management started in 1998 when current Chief Executive Officer (CEO) Tim Cook came to Apple as the senior vice president of worldwide operations. He immediately reduced the number of suppliers from 100 to 24, resulting in better deals for Apple, shrunk inventory turnover time from months to days, and cut production time for Apple computers in half.[12] Apple also uses innovative measures like shredding old iPhones to prevent components from being utilized in counterfeit phones.[13]

Another model for comparison is the United Kingdom's Ministry of Defence (MoD) procurement system. The UK MoD procurement structure is significantly different from its counterpart in the United States in that one organization is responsible for the acquisition of weapons systems and military equipment required by all branches of its armed forces.[14] The UK MoD utilizes a "Smart Acquisition" initiative, which implements a through-life approach to procurement rather than primarily focusing resources on the initial purchase.[15] Through the use of Smart Acquisition, the MoD seeks to integrate its individual resources into overarching systems rather than simply replacing resources on a one-for-one basis.[16] The UK MoD also works to build long-term

---

[11] "Gartner Supply Chain Top25," June 3, 2017, http://www.gartner.com/technology/supply-chain/top25.jsp.

[12] Paul Simpson, "Tim Cook: The 'Cool Customer' Behind Apple's Supply Chain Success," Supply Management, January 18, 2016, https://www.cips.org/supply-management/analysis/2016/february/tim-cook-the-cool-customer-behind-apples-supply-chain-success/.

[13] Kif Leswing, "Apples 'Shreds" Old iPhones to Prevent Real Parts from Ending up in Fakes," *Business Insider*, February 17, 2016, http://www.businessinsider.com/apple-shreds-old-iphones-to-prevent-real-parts-ending-up-in-fakes-2016-2,

[14] Martin Auger, *Defense Procurement Organizations: A Global Comparison*, Publication No.2014-82-E (Ottawa, Canada: Library of Parliament, 2014), https://lop.parl.ca/Content/LOP/ResearchPublications/2014-82-e.pdf.

[15] Bernard Gray, "Review of Acquisition for the Secretary of State for Defense" (independent report, BiP Solutions, 2009), https://www.bipsolutions.com/docstore/ReviewAcquisitionGrayreport.pdf.

[16] Jacques S. Gansler, William Lucyshyn, and Lisa H. Harrington, "An Analysis of Through Life Support Capability Management at the U.K.'s Ministry of Defense" (report, University of Maryland Center for Public Policy and Private Enterprise, 2012), https://www.dau.mil/cop/pbl/DAU%20Sponsored%20Documents/UMD%20FINAL%20Report%20LMCO%20An%20Analysis%20of%20Through%20Life%20Support%20Capability%20Management%20at%20the%20UK%20s%20Ministry%20of%20Defense%20June%202012.pdf.

collaborative relationships with industry stakeholders, resulting in a shared risk model, which increases the level of responsibility assumed by industry, thereby providing an impetus for industry to be more responsive.[17] This practice starkly contrasts the current Department of Defense (DOD) methodology, which utilizes an enforcement-based regulatory approach.

By utilizing these two industry leading models, this thesis has identified two sets of well-documented and validated best practices to serve as examples. The intent of this thesis is to provide a comparative analysis of these two distinctive organizations, and the respective supply chain management practices, to identify the policies and methodologies they use to ensure the integrity of their supply chains. In so doing, the thesis seeks to determine what measures can be applied to the U.S. defense supply chain to reduce or eliminate counterfeit electronic components.

C. RESEARCH DESIGN

I started this research by reviewing the DOD procurement system and the problem of counterfeit components in the defense supply chain. Then I conducted a multiple case study by reviewing the supply chain management practices of Apple and the UK MoD. By analyzing what makes these supply chains successful, the respective structures, practices, and policies can be applied to the DOD procurement process to reduce the number of counterfeit components in the defense supply chain.

This thesis employs a comparative case study methodology to assess how two different organizations prevent counterfeit components from entering their supply chains. As Robert K. Yin identifies in his often-cited work, *Case Study Research: Design and Methods*, "How and why questions are more explanatory and likely to lead to the use of a case study."[18] The two cases, Apple and the UK Mod, were identified as candidates while I researched the DOD's counterfeit component epidemic. The organizations were ultimately selected because they contain similar processes, policies, and methodologies. Furthermore, these determining factors provide a distinct contrast to the practices

[17] Gansler, Lucyshyn, and Harrington, "Through Life Support Capability Management."

[18] Robert K. Yin, *Case Study Research: Design and Methods* (Los Angeles: SAGE, 2014), 10.

employed by the DOD. This research method allowed me to assess multiple practices across the two entities' operations. These practices include the organization's level of integration within supply chain management strategies, and use of collaboration, contracting methods, and policies.

D. LITERATURE REVIEW

There is extensive literature on the issue of counterfeit components and the defense supply chain. However, the emphasis of this material is on the identification of the problem, subsequent regulatory changes, and the response of industry. The intent of this thesis is to identify the best practices and policies of supply chain management from industry leaders Apple and the United Kingdom's Ministry of Defence (MoD). In line with the focus of this thesis, the literature review starts by examining the defense supply chain, its governing regulations, and changes in the industry. It then considers the issues of counterfeiting, the increased presence of counterfeits in the supply chain, and the response to this epidemic. The review culminates with an examination of the practices and policies utilized by Apple and the MoD.

1. The Defense Supply Chain

As is the case with most government entities, the defense supply chain is more complicated than the standard supply chain. The usual layers of bureaucracy are further complicated by the number and complexity of regulations surrounding government contracts and contracting officers, as well as by the different levels of procurement and acquisition. The varying levels of procurement include sole source procurement, multiple award contracts, normal procurements, simplified acquisitions, and purchases over $25,000.[19] All of these activities and other forms of DOD procurement activities are administered by three different sets of regulations: the Federal Acquisition Regulation,

[19] Michael Barne, "Overview of the DOD Procurement Process," ThoughtCo., August 10, 2016, https://www.thoughtco.com/overview-dod-procurement-process-1052245.

the Defense Federal Acquisition Regulation Supplement, and the component-unique Federal Acquisition Regulation Supplements.[20]

Just as manufacturing and supply chains have become much more globalized, so too have the sources for the defense supply chain. While this has afforded the United States the opportunity to obtain superior technologies, products, and management techniques, the question is: At what cost?[21] The Alliance for American Manufacturing answered this very question when it released a report in May 2013 which indicated that dependence on foreign suppliers was putting the defense supply chain and national security at risk.[22] According to the report, the United States now relies on a single Chinese source for solid rocket fuel and sources 91 percent of a rare-earth element from China.[23] The report also indicated that U.S.-developed technologies are no longer produced in the United States; in fact, "the number of major U.S.-based defense and aerospace companies shrunk from 21 in 1993 to six [in 2014]."[24] As a result of the increased dependence on foreign sources, every U.S. weapons system likely contains foreign-made parts.

2. Counterfeits and the Defense Supply Chain

While advanced technology and manufacturing have allowed criminal organizations to counterfeit any category of commodity, including military-grade components, the counterfeiting phenomenon is not a new one. The Roman author and philosopher Pliny the Elder (23–79 AD) addressed in great detail the issues of fraud and

---

[20] Moshe Schwartz, *Defense Acquisitions: How DOD Acquires Weapons Systems and Recent Efforts to Reform the Process*, CRS Report No. RL34026 (Washington, DC: Congressional Research Service, 2014), https://fas.org/sgp/crs/natsec/RL34026.pdf.

[21] Theodore H. Martin, "The Globalization of America's Defense Industries: Managing the Threat of Foreign Dependence," *International Security* 15, n.o. 1 (Summer 1990): 57–99, https://www.jstor.org/stable/pdf/2538982.pdf?refreqid=excelsior%3A1188b7db5e859981aed8817ca6ba5440.

[22] John Adams, *Remaking American Security: Supply Chain Vulnerabilities & National Security Risks across the U.S. Defense Industrial Base* (Washington, DC: Alliance for American Manufacturing, 2013), http://s3-us-west-2.amazonaws.com/aamweb/uploads/research-pdf/RemakingAmericanSecurityMay2013_2.pdf.

[23] Ibid.

[24] Ibid.; Jacques S. Gansler, William Lucyshyn, and John Rigilano, "Addressing Counterfeit Parts in the DOD Supply Chain" (report, University of Maryland Center for Public Policy and Private Enterprise, 2014), 7, https://calhoun.nps.edu/bitstream/handle/10945/45074/UMD-LM-14-012.pdf?sequence=1.

counterfeiting in his book on natural history, in which he discussed attempts to counterfeit opals and other precious stones.[25] He also addressed the early attempts to counterfeit coins, explaining that some collectors prized the fakes over their real counterparts. In more recent history, according to William Eleroy Curtis, "The superiority of American [cotton] goods is so great that the Manchester [England] mills send few goods to South America that do not bear forged American trademarks."[26] Accordingly, counterfeiting has become a thriving global enterprise that often funds organized crime and terrorist organizations alike.[27]

The Organization for Economic Cooperation and Development (OECD), in its 2016 study *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact*, "estimates that global trade-related counterfeiting accounts for 2.5 percent of world trade, or $461 billion."[28] This reflects an increase of 0.6 percent in the growth of global counterfeiting from the OECD's 2008 study, or an additional $211 billion.[29] The U.S. Government Accountability Office (GAO) reports that, as a result of counterfeiting, "The U.S. economy as a whole may grow more slowly because of reduced innovation and the loss of trade revenue."[30] Additionally, the OECD indicates that there have been both a shift and expansion in the types of products being counterfeited.[31] This expansion of counterfeit products can be seen through enforcement actions undertaken to interdict fake electronics. Two of the initial efforts include operations Cisco Raider and Network

---

[25] John Bostock, *Pliny the Elder, The Natural History* (London: Taylor and Francis, 1855), http://www.perseus.tufts.edu/hopper/text?doc=Perseus:abo:phi,0978,001:33.

[26] Peggy Chaudhry and Alan Zimmerman, *Protecting Your Intellectual Property Rights* (New York: Springer-Verlag, 2013), 9.

[27] Stafano Betti and Rosella Mangion, "Prosecuting Counterfeiting and Organised Crime: The Need for a Creative Legal Approach," in *Anti-counterfeiting 2014: A Global Guide* (World Trademark Review, 2014).

[28] Organization of Economic Cooperation and Development, *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact* (Paris: OECD Publishing, 2016), 11.

[29] Ibid.

[30] Government Accountability Office (GAO), *Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*, GAO-10-423 (Washington, DC: GAO, 2010), introduction.

[31] Chaudhry and Zimmerman, *Protecting Your Intellectual Property Rights*.

Raider, as identified by the Federal Bureau of Investigation (FBI).[32] These actions specifically targeted counterfeit network hardware such as network routers, switches, network cards, and modules manufactured by Cisco and other well-known companies. The results of the two operations included the issuance of more than thirty-five search warrants and forty convictions, and the seizure of $220 million in counterfeit network hardware.[33]

The issue of counterfeit components in the defense supply chain came to a head in 2011 during a Senate Armed Services Committee investigation, when a number of large defense contractors reported 1,800 cases, covering one million parts, of suspected counterfeit parts.[34] The Senate Armed Services Committee investigation identified vulnerabilities throughout the supply chain that allowed counterfeit parts to infiltrate crucial defense systems, finding that 70 percent of all counterfeits came from China, where there were entire factories engaged in counterfeiting electronic components.[35] In the same investigation, the Semiconductor Industry Association reported that the theft of intellectual property by Chinese counterfeiters has cost its industry an estimated $7.5 billion annually in lost revenue.[36] The Semiconductor Industry Association, which employs nearly 200,000 American workers, also reported that this theft has cost U.S. workers almost 11,000 jobs annually.

The GAO initiated a subsequent investigation in 2012, with the intent to determine the availability of counterfeit parts on Internet platforms commonly used to

---

[32] "Departments of Justice and Homeland Security Announce 30 Convictions, More than $143 Million in Seizures from Initiative Targeting Traffickers in Counterfeit Network Hardware," Department of Justice, May 6, 2010, https://www.justice.gov/opa/pr/departments-justice-and-homeland-security-announce-30-convictions-more-143-million-seizures.

[33] "China Syndrome: Operation Targeting Counterfeit Network Hardware from China Yield Convictions, Seizures," Homeland Security Newswire, May 21, 2010, www.homelandsecuritynews wire.com/operation-targeting-counterfeit-network-hardware-china-yield-convictions-seizures?page=0,2.

[34] Senate Committee on Armed Services, *Counterfeit Electronic Parts*.

[35] Ibid.

[36] Ibid.

purchase military-grade electronics.[37] As part of its investigation, the "GAO created a fictitious company and gained access to two Internet platforms providing access to vendors selling military-grade electronic parts."[38] These efforts allowed the GAO to purchase sixteen requested parts, all of which were determined to be counterfeit, from multiple vendors in China.[39] Through the use of authentication testing, it was determined that twelve of the sixteen "parts had been re-marked to display the part numbers and manufacturer logos of authentic parts."[40] Of the remaining parts purchased by the GAO, all were determined to have completely fictitious parts numbers, demonstrating the counterfeiters' lack of knowledge.[41]

In response to the epidemic of counterfeit parts in the defense supply chain and the threat they posed to national security, a bipartisan amendment was introduced into the Fiscal Year 2012 National Defense Authorization Act.[42] As discussed in more detail in Chapter III, the amendment was passed as section 818 of the final Act and signed into law on December 31, 2011. The enactment required the DOD to issue regulations and guidance to address the detection and avoidance of counterfeit electronic parts.

On May 6, 2014, the DOD issued a final rule regarding the detection and avoidance of counterfeit electronic parts, amending the Defense Federal Acquisition Regulation Supplements.[43] The final rule provided the definitions for counterfeit electronic parts, suspect counterfeit parts, electronic parts, and obsolete electronic parts as

---

[37] Richard J. Hillman, *DOD Supply Chain: Preliminary Observations Indicate that Counterfeit Electronic Parts Can be Found on Internet Purchasing Platforms*, GAO-12-213T (Washington, DC: GAO, 2011), http://www.gao.gov/assets/590/586136.pdf.

[38] GAO, *DOD Supply Chain: Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms*, GAO-12-375 (Washington, DC: GAO, 2012), introduction, http://gao.gov/products/GAO-12-375.

[39] GAO, *DOD Supply Chain*.

[40] Ibid.

[41] Ibid.

[42] American Bar Association Public Contract Law Section, "A White Paper Regarding Department of Defense Implementation of Section 818 of the National Defense Authorization Act for Fiscal Year 2012" (white paper, American Bar Association, 2012).

[43] "Comment on FR Doc # 2013-11400," Regulations.gov, May 5, 2014, accessed December 10, 2016, https://www.regulations.gov/document?D=DARS-2013-0014-0044.

required by section 818.[44] However, implementation of the final rule did little to address the lack of incentive for suppliers to comply with the required reporting process, as the cost of any remediation is borne by the supplier. It also failed to address the DOD's lack of guidance to contractors and subcontractors as to what constitutes an "acceptable counterfeit electronic part avoidance and detection system," as required by Defense Federal Acquisition Regulation Supplement 246.870-2.[45]

3. Apple and the United Kingdom's Ministry of Defence: Industry Leaders in Supply Chain Management

The primary function of supply chain management is to manage the multiple upstream and downstream flows within in the supply chain, including products, services, information, finances, demand, relationships, and risks. In a more complete definition, supply chain management is "the systemic, strategic coordination of the traditional business functions and the tactics across these business functions within a particular company and across businesses within the supply chain, for the purposes of improving the long term performance of the individual companies and the supply chain as a whole."[46] Significantly, this definition emphasizes the coordination across all business functions within a company and across the supply chain as a whole. This is best exemplified through Apple's approach to supply chain management, whereby the performance of a microprocessor and a customer's product buying experience at an Apple store are intrinsically linked.[47]

Apple has been ranked number one in supply chain management by Gartner Research since 2008 and was placed in Gartner's elite masters category in 2015.[48] The rise to industry leader in supply chain management and the obstacles Apple overcame are documented across a range of sources, including Walter Issacson's biography of Steve

---

[44] Ibid.

[45] "3 Problems In DOD Counterfeit Parts Rule," Law 360, August 27, 2013, www.law360.com/articles/468034/3-problems-in-dod-counterfeit-parts-rule.

[46] John T. Mentzer et al.," *Journal of Business Logistics* 22, no. 2 (September 2001): 11.

[47] "7 Supply Chain Lessons from Steve Jobs," Supply Chain 24–7, September 3, 2013, http://www.supplychain247.com/article/7_supply_chain_lessons_from_steve_jobs

[48] "Gartner Supply Chain Top25."

Jobs, newspapers articles, industry websites, and industry journals. Issacon's biography is the only inside look into Apple—and into Jobs himself—that has been authorized by Jobs. The book is based on more than forty interviews between Jobs and Issacson that were conducted over a two-year period.[49] There were also numerous interviews with colleagues, friends, family members, competitors, and adversaries that helped provide a complete picture of the company and the man behind it.[50] The newspaper articles highlight some of the controversy associated with Apple's success. For instance, a 2012 *New York Times* article identified a number of labor issues at the Foxconn facilities in China, where Apple iPhones are assembled.[51] The industry websites and journals provide another perspective of the company and its practices—for example, the January 2016 issue of *Supply Management* illustrates how the work of Apple's current CEO Tim Cook was key to the success of its supply chain management strategy.[52]

My review of the MoD began with a publication from the Canadian Library of Parliament titled *Defense Procurement Organizations: A Global Comparison*, issued in 2014.[53] The report identifies the structural and policy differences between defense procurement agencies across the globe. In doing so, it provides the initial foundation on which to compare the U.S. defense supply chain to that of United Kingdom's. A subsequent source was an independent report produced by Bernard Gray, titled "Review of Acquisition for the Secretary of State for Defense"; Gray's report highlights the MoD policy of Smart Acquisition, which uses a through-life approach for defense procurement.[54] Another document used to analyze the MoD's through-life practice, issued by the University in Maryland in 2012, was titled "An Analysis of Through-Life

---

[49] Walter Issacson, *Steve Jobs*, e-book (New York: Simon Schuster, 2011), introduction.

[50] Ibid.

[51] Charles Duhigg and Keith Bradsher, "How The U.S. Lost out on iPhone Work," *New York Times*, January 21, 2012, http://www.nytimes.com/2012/01/22/business/apple-america-and-a-squeezed-middle-class.html.

[52] Simpson, "Tim Cook."

[53] Auger, *Defense Procurement Organizations*.

[54] Gray, "Review of Acquisition."

Support—Capability Management at The U.K.'s Ministry of Defense."[55] Other sources consulted included the MoD's webpage, reports, and policy papers such the Defence Standard 05-135: *Avoidance of Fraudulent Materiel*.[56] The Defence standard identifies the parameters by which MoD suppliers are measured to show they are managing the risk of counterfeit parts and preventing the delivery of said parts to the MoD.

[55] Gansler, Lucyshyn, and Harrington, "Through-Life Support."

[56] Ministry of Defense, *Avoidance of Counterfeit Materiel*, DEF STAN 05-135 (Glasgow, UK: Defence Equipment and Support, 2014).

II. DEPARTMENT OF DEFENSE PROCUREMENT BACKGROUND

The DOD procurement and acquisition process epitomizes bureaucracy with its multiple agencies, sub-agencies, legions of civilian and military employees, and a plethora of regulations. It is in this environment that the problem of counterfeit electronic components has been allowed not only to occur, but to reach epidemic levels. This chapter examines the DOD procurement process, counterfeits in the supply chain, and the response to the problem of counterfeit components.

A. DEPARTMENT OF DEFENSE PROCUREMENT

While defense procurement and acquisition in the United States is managed by the DOD, each of the individual armed services is ultimately responsible for its own acquisition needs and is supported by distinct procurement offices. The Office of the Assistant Secretary of the Navy Research, Development, and Acquisition oversees U.S. Navy and U.S. Marine Corps procurement. The Office of the Assistant Secretary of the Army Acquisition, Logistics, and Technology oversees U.S. Army procurement, and the Office of the Assistant Secretary of the Air Force Acquisition is responsible for U.S. Air Force Procurement.[57] Each of these offices, along with the DOD, has a number of subordinate organizations that are involved in purchasing, many of which specialize in unique fields of procurement—from weapons acquisition, to the purchase of commercial products, to support services.[58] In total, the DOD is made up of twenty-two different acquisition agencies that comprise more than 136,000 military and civilian personnel.[59]

In addition to the numerous procurement agencies that compose the DOD, there are multiple layers of regulation. These include the Federal Acquisition Regulation, Defense Federal Acquisition Regulation Supplement, and the component-unique Federal

---

[57] Auger, *Defense Procurement Organizations*.

[58] Ibid.

[59] Susan M. Gates et al., *Analyses of the Department of Defense Acquisition Workforce: Update to Methods and Results through FY 2011* (Santa Monica, CA: RAND, 2013), 4, http://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR110/RAND_RR110.pdf.

Acquisition Regulation Supplements.[60] The Federal Acquisition Regulation, or FAR, covers the acquisition of all materials and services by executive agencies; it "precludes agency acquisition regulations that unnecessarily repeat, paraphrase, or otherwise restate the FAR, limits agency acquisition regulations to those necessary to implement FAR policies and procedures within an agency, and provides for coordination, simplicity, and uniformity in the Federal acquisition process."[61] The defense supplement contains requirements of law, DOD-wide policies, and delegations and deviations from Federal Acquisition Regulation authorities and requirements, and is used to implement and supplement the regulation.[62] The component-unique supplements are regulations specific to each branch of the military and add an additional layer of bureaucracy for procurement personnel to navigate.

B. IDENTIFICATION OF COUNTERFEITS IN THE DEFENSE SUPPLY CHAIN

As part of a 2011 Senate Armed Services Committee investigation into counterfeit electronic parts in the DOD supply chain, a number of large defense contractors reported 1,800 cases—covering one million pieces—of suspected counterfeit parts.[63] In the same report, the Semiconductor Industry Association identified that the theft of intellectual property by Chinese counterfeiters had cost their industry an estimated $7.5 billion per year in lost revenue.[64]

The Armed Services Committee investigation also identified "that vulnerabilities throughout the defense supply chain allow counterfeit electronic parts to infiltrate critical U.S. Military Systems, risking our security and the lives of the men and women who protect it."[65] As previously mentioned, the investigation found that 70 percent of all

---

[60] Schwartz, *Defense Acquisitions*.

[61] Federal Acquisition Regulation, vol.1, parts 1–51 (2005).

[62] "Defense Federal Acquisition Regulations Supplements," Federal Register, accessed July 12, 2017, https://www.federalregister.gov/defense-federal-acquisition-regulation-supplement-dfars-.

[63] Senate Committee on Armed Services, *Counterfeit Electronic Parts*.

[64] Ibid.

[65] Ibid.

counterfeits come from China, where there are entire factories set up for the purpose of counterfeiting electronic components.[66] Of the remaining 30 percent, a significant portion can also be linked to China when traced back through the supply chain. The ice detection module in the Navy's P-8A Poseidon aircraft was just one of many examples cited in the report for having counterfeit parts.[67] After BAE Systems sold the aircraft to the Navy, as previously discussed, the company discovered that components in the modules, which they had believed were newly manufactured, were actually used parts that had been sanded down, resurfaced, and remarked to appear new.[68] When traced through the supply chain, it was determined that the counterfeit parts came from a U.S. supplier who originally purchased them from A Access Electronics in Shenzhen, China.[69]

The Institute of Electrical and Electronics Engineers (IEEE) also narrowed in on the technique of sanding and resurfacing components in its 2008 Annual Technology Report.[70] The report found that, historically, counterfeits are "clones" or copies of high-value components; however, as the electrical industry has matured and an increasing number of united have grown obsolete, opportunities for counterfeiters have expanded.[71] These increased opportunities have allowed counterfeiters to leverage traditional methods, such as re-marking the product type or speed of high-end components. Figure 1 shows an example of a resurfaced integrated circuit from the IEEE report.[72]

---

66 Senate Committee on Armed Services, *Counterfeit Electronic Parts*.

67 Ibid.

68 Ibid.

69 Ibid.

70 IEEE, "IEEE Reliability Society Technical Operations Annual Technology Report for 2008," *IEEE Transactions on Reliability* 58, no. 2 (June 2009): 210–261, http://ieeexplore.ieee.org/document/5062554/.

71 Ibid.

72 Ibid.

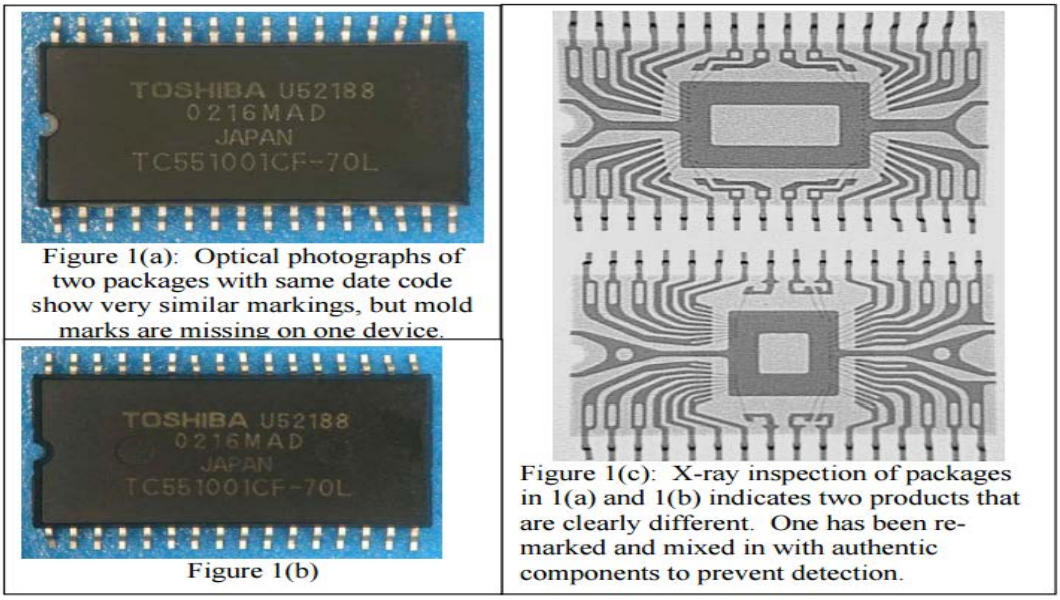


Figure 1. Counterfeit Integrated Circuit[73]

The GAO initiated a subsequent investigation into the counterfeit parts in 2012. Honing in on counterfeit parts commonly used in military-grade electronics, the GAO sought to determine the availability of these counterfeit parts on Internet platforms.[74] To gain access to Internet platforms, the GAO created a fictitious company and then requested quotes for sixteen different parts. The requests were divided into "three categories: (1) authentic part numbers for obsolete and rare parts; (2) authentic part numbers with post-production date codes (date codes after the last date the part was manufactured); and (3) bogus, or fictitious, part numbers that are not associated with any authentic parts."[75] Based on its requests, the GAO received 396 responses, 334 of which originated from China.[76] In accordance with the selection criteria established by the GAO, all sixteen parts were purchased from vendors in China.[77] Of the sixteen parts purchased, twelve were classified within category 1—rare part numbers—and category

[73] Source: IEEE, "Technical Operations Annual Technology Report," 238.

[74] Hillman, *DOD Supply Chain*.

[75] GAO, *DOD Supply Chain*.

[76] Ibid.

[77] Ibid.

2—post-production date codes; all were identified as suspect counterfeit by the testing lab.[78] Multiple authentication tests determined "that the parts had been re-marked to display the part numbers and manufacturer logos of authentic parts."[79] For the parts from category 3—bogus or fictitious parts numbers—the GAO purchased four parts from four different vendors, demonstrating both the counterfeiters' lack of knowledge and willingness to profit from the shoddy parts.[80]

As further evidence of the threat counterfeit parts pose to the supply chain, a great number of enforcement actions—with a wide scope—have been undertaken to interdict counterfeit components. Two of the initial efforts included FBI operations "Cisco Raider" and "Network Raider."[81] These actions specifically targeted "the illegal importation and sale of counterfeit network hardware, in particular network routers, switches, network cards, and modules manufactured by Cisco," and other well-known companies.[82] Both operations were international, multiagency efforts that included the FBI, Homeland Security Investigations, Customs and Border Protection (CBP), the Royal Canadian Mounted Police, the Canadian Border Services Agency, the Defense Criminal Investigative Service, and the Internal Revenue Service (IRS).[83] The initial phases of these efforts began as early as 2005, when CBP and Homeland Security Investigations opened multiple investigations in seventeen separate field offices.[84] These operations resulted in "30 felony convictions and more than 700 seizures of counterfeit Cisco network hardware and labels with an estimated retail value of more than $143 million."[85]

---

[78] GAO, *DOD Supply Chain*.

[79] Ibid., introduction.

[80] Ibid.

[81] Department of Justice, "Counterfeit Network Hardware."

[82] Michael Cooney, "Taskforce Seizes $76 Million in Counterfeit Cisco Network Hardware," Network World, February 29, 2008, http://www.networkworld.com/article/2237296/security/taskforce-seizes--76-million-in-counterfeit-cisco-network-hardware.html.

[83] Ibid.

[84] Ibid.

[85] Homeland Security Newswire, "China Syndrome: Operation."

These operations were followed by another collaborative international effort between CBP and the European Union Commission Tax and Customs Directorate. Between November and December 2007, the agencies participated in their first joint anti-counterfeiting enforcement effort, dubbed "Operation Infrastructure," which targeted integrated chips and computer components.[86] The operation resulted in the seizure of "integrated circuits and computer components of over 40 trademarks including Intel, Cisco, and Philips, worth more than $1.3 billion."[87] Based on the success of the operation and a request from the Semiconductor Industry Association, "Operation Infrastructure II" was conducted the following spring. The subsequent action resulted in the seizure of 420,000 integrated circuits and computer components.[88] These efforts' successes were lauded by Minister Counselor Francois Rivasseau, deputy chief of mission for the French Embassy, at a 2008 trade symposium, where he declared that part of the European Union response to intellectual property theft was developing international cooperation among enforcement authorities.[89]

C. THE RESPONSE TO COUNTERFEITS IN THE DEFENSE SUPPLY CHAIN

In response to the rising tide of counterfeit parts in the defense supply chain, as highlighted by the Senate Armed Services Committee investigation and the resulting hearing, a bipartisan amendment was introduced to the Fiscal Year 2012 National Defense Authorization Act.[90] The intent of the amendment was to "stop the importation of counterfeit electronic parts into the United States, address weaknesses in the defense

---

[86] "Remarks by Minister Counselor Francois Rivasseau, Deputy Chief of Mission, Embassy of France to the USA, U.S. Customs and Border Protection," U.S. Customs and Border Protection (CBP), October 31, 2008, https://www.cbp.gov/trade/stakeholder-engagement/trade-symposium/2008-trade-symposium/event-materials/francois-speech.

[87] "EU, U.S. Vow Crackdown on Computer Counterfeits," Reuters, February 22, 2008, https://www.reuters.com/article/us-eu-usa-counterfeiting/eu-u-s-vow-crackdown-on-computer-counterfeits-idUSL2285388920080222.

[88] Daryl Hatano, "SIA OMB IP Enforcement Joint Strategic Plan," Semiconductor Industry Association, March 23, 2010, http://www.semiconductors.org/clientuploads/directory/DocumentSIA/Anti Counterfeiting Task Force/SIA OMB IP enforcement joint strategic plan FINAL 0310.pdf.

[89] CBP, "Remarks by Minister Counselor Francois Rivasseau."

[90] American Bar Association Public Contract Law Section, "Section 818."

supply chain and to promote the adoption of aggressive counterfeit avoidance practices by the DOD and the defense industry."[91] The amendment was passed as section 818 of the Fiscal Year 2012 National Defense Authorization Act when President Obama signed House Resolution 1540 into law on December 31, 2011.

1. Section 818

Section 818 required the DOD to issue regulations and guidance and to establish processes to address the detection and avoidance of counterfeit electronic parts. The first of these actions, in accordance with subsection (b)(1), was to establish department-wide definitions for the term *counterfeit electronic parts*.[92] While establishing uniform definitions for DOD suppliers and contractors was a step in the right direction, it is a redundant step for imported products; existing sections within 18 and 19 United States Code already define counterfeits and identify sanctions for persons who import counterfeit goods.

The next crucial requirement of section 818 was for the DOD, as described in subsections (b)(4) and (c)(4), to establish guidelines for department personnel, contractors, and subcontractors to report suspected counterfeit parts in writing to the appropriate government authorities and the Government-Industry Data Exchange Program. These sections read as follows:

> (b)(4) establish processes for ensuring that Department personnel who become aware of, or have reason to suspect, that any end item, component, part, or material contained in supplies purchased by or for the Department contains counterfeit electronic parts or suspect counterfeit electronic parts provide a report in writing within 60 days to appropriate Government authorities and to the Government-Industry Data Exchange Program (or a similar program designated by the Secretary);
>
> (c)(4) REPORTING REQUIREMENT.—The revised regulations issued pursuant to paragraph (1) shall require that any Department contractor or subcontractor who becomes aware, or has reason to suspect, that any end item, component, part, or material contained in supplies purchased by the Department, or purchased by a contractor or subcontractor for delivery to,

[91] American Bar Association Public Contract Law Section, "Section 818," 7.

[92] National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112–81, § 818(b)(1) (2012).

> or on behalf of, the Department, contains counterfeit electronic parts or suspect counterfeit electronic parts report in writing within 60 days to appropriate Government authorities and the Government-Industry Data Exchange Program (or a similar program designated by the Secretary).[93]

As a means to increase compliance with the reporting requirement for contractors and subcontractors, subsection (c)(5) identifies that contractors or subcontractors will not face any civil liability for the reporting of counterfeit or suspect counterfeit items.[94]

Mandating the reporting of counterfeits or suspected counterfeits while alleviating civil liability is a necessary step to address the problem. However, it lacks the incentive needed for contractors or subcontractors to follow through on the required reporting process. As businesses, contractors are more concerned with their bottom line; without a financial incentive to report counterfeit components, the process lacks sustainability. The poor incentivization is further exacerbated in subsection (c)(2)(B), which specifically states that the cost to replace or corrective action to remedy the issues associated with counterfeit parts is not considered an allowable cost under DOD contracts.[95]

In an effort to address these concerns, section 833 of the Fiscal Year 2013 National Defense Authorization Act amended section 818(c)(2)(B) to allow "certain protections for contractors performing rework or corrective action to remedy the use of counterfeit electronic parts," provided that they met the identified criteria.[96] While this subsection sought to remedy the situation, its first requirement fell short, stating, "The covered contractor has an operational system to detect and avoid counterfeit parts and suspect counterfeit electronic parts." The DOD has yet to provide guidance for what constitutes an "acceptable counterfeit electronic part detection and avoidance system," as required under 48 CFR 246.870-2(b)(1).[97]

---

[93] National Defense Authorization Act for Fiscal Year 2012, 818(b)(4), (c)(4).

[94] Ibid., 818(c)(5).

[95] Ibid., 818(c)(2)(B).

[96] "President Obama Signs FY2013 National Defense Authorization Act," Lexology, January 4, 2013, https://www.lexology.com/library/detail.aspx?g=b9717837-8fe2-4862-97df-a776f12ea9d6.

[97] Federal Acquisition Regulation System, 48 C.F.R.§ 246.870-2 (2016), https://www.law.cornell.edu/cfr/text/48/246.870-2.

2. Final Rule

Effective May 6, 2014, the DOD issued a final rule amending the Defense Federal Acquisition Regulation Supplement, regarding the detection and avoidance of counterfeit electronic parts.[98] The final rule defined counterfeit electronic parts, suspect counterfeit parts, electronic parts, and obsolete electronic parts, as described by section 818 of the Fiscal Year 2012 National Defense Authorization Act:

> Counterfeit electronic part means 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.
>
> Electronic part means an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly (section 818(f)(2) of Pub. L. 112–81). The term "electronic part" includes any embedded software or firmware.
>
> Obsolete electronic part means an electronic part that is no longer in production by the original manufacturer or an aftermarket manufacturer that has been provided express written authorization from the current design activity or original manufacturer.
>
> Suspect counterfeit electronic part means an electronic part for which credible evidence (including, but not limited to, visual inspection or testing) provides reasonable doubt that the electronic part is authentic.[99]

During the final rule review period, it was determined that the required reporting of counterfeit components would occur through the Government-Industry Data Exchange Program.[100]

---

98 "Comment on FR Doc # 2013-11400."

99 Ibid.

100 Ibid.

Even the implementation of the final rule did not address the lack of incentives for suppliers to comply with the required reporting process. It also failed to address the DOD's lack of guidance to contractors and subcontractors for what constitutes an "acceptable counterfeit electronic part detection and avoidance system," as discussed in 48 CFR 246.870-2(b)(1).[101]

3. Review of Reporting Process

In 2016, the GAO conducted a review of the DOD reporting process to examine the Government-Industry Data Exchange Program reporting mechanism. The review also served to determine the reporting system's "effectiveness as an early warning system" and the "DOD's assessment of defense contractors' systems for detecting and avoiding counterfeits."[102] In its review of the mandatory reporting for suspect counterfeit parts, the GAO determined the DOD's implementation efforts have limited the Government-Industry Data Exchange Program's effectiveness as an early warning system.[103] The identified issues include a lack of DOD oversight to ensure reporting as required, "no standardized process for establishing how much evidence is needed before reporting suspect counterfeit parts," and a lack of transparency in reporting, which limits the ability to make industry partners aware of possible counterfeits or suspected tends.[104] The report also determined that all contractors reviewed by the GAO "have established systems to detect and avoid counterfeit electronic parts," as required by section 818.[105] However, the DOD still did not implement guidance for how these systems should be reviewed, assessed, or validated.

---

[101] Federal Acquisition Regulation System, 48 C.F.R.§ 246.870-2.

[102] GAO, *Counterfeit Parts: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk*, GAO-16-236 (Washington, DC: GAO, 2016). https://www.gao.gov/assets/680/675227.pdf.

[103] Ibid.

[104] Ibid.

[105] Ibid.

4. Industry Concerns

While there is agreement across the industry that counterfeit electronic components are a significant threat to the defense supply chain and that the final rule is the most effective means to address the issue, industry still has a number of concerns with the final rule.[106] In late 2014, a group of industry thought leaders convened a panel to address the issues facing defense contractors, and identified the following concerns:

> The Defense Federal Acquisition Regulation Supplement contains 25 other criteria, several of which subsume the 12 policies and procedures contained within the final rule.
>
> The expanded definition of counterfeit/suspect counterfeit electronic parts includes embedded software and firmware, which are historically difficult to detect as counterfeits.
>
> The lack of guidance regarding measures contractors should take to "control" obsolete parts or electronic parts that are no longer in production by the original manufacturer.
>
> The DOD's failure to describe standards and criteria used to evaluate contractor systems for compliance in developing adequate avoidance and detection.[107]

The defense supply chain is inundated with counterfeit electronic components and the response has been incomplete at best. This begs the question: What measures would be effective in securing the defense supply chain? The following chapters examine two very different organizations, Apple and the United Kingdom's MoD, and their supply chain management structures and practices. In so doing, these chapters seek to identify the key practices and philosophies that can be used to improve and protect the U.S. defense supply chain.

---

[106] Vincent J. Napolean and Diana Vilmenay, "Insights on DOD's Final Counterfeit Parts Rule," Law360, December 15, 2014, http://www.law360.com/articles/604164/insights-on-dod-s-final-counterfeit-parts-rule.

[107] Ibid.; GAO, *Counterfeit Parts*.

THIS PAGE INTENTIONALLY LEFT BLANK

III. APPLE: *THE* INDUSTRY LEADER IN SUPPLY CHAIN MANAGEMENT

In the mid- to late 1970s, the use of personal computers was limited to technology enthusiasts and hobbyists capable of assembling the computer themselves from individual components or premade kits. Already assembled, off-the-shelf personal computers as we know them today had not yet come to fruition. It was during this period that Steve Jobs, Steve Wozniak, and Ronald Wayne founded Apple Computers Company with the goal of manufacturing and selling premade personal computers. To achieve this goal it would take more than their knowledge and passion for computers. It would also take a shrewd business sense, which would ultimately become one of Apple's—not to mention Steve Jobs'—hallmarks. To understand what makes Apple number one in supply chain management, and thus an exemplar for the defense supply chain, this chapter reviews the company's practices and policies including new product development, procurement, product assembly, and logistics, all of which contribute to its continued success.

A. APPLE'S ORIGINS

With the success of its first product, the Apple I, Apple, under the guidance of Steve Jobs, demonstrated a business prowess that foreshadowed the company's future. To facilitate the development and first sale of its product (fifty units to a local computer store called the Byte Shop), Jobs negotiated a 30-day credit agreement with his supplier, Cramer Electronics.[108] Within about a year, Apple was able to sell 200 Apple I computers to other stores and individual hobbyists. The successful launch of this initial product line was based on the credit agreement with Cramer as well as Jobs' ability to negotiate a better price for the components needed to build the computers.[109]

Even with the success of its initial product launch, Apple needed to find new partners to help finance its next product line. To fulfill this need, Mike Markkula, who

[108] Issacson, *Steve Jobs*, chapter 5.

[109] Ibid.

agreed to provide a $250,000 line of credit, became a one-third partner in Apple.[110] This line of credit allowed Jobs to create the Apple II, which was a fully integrated personal computer that emphasized the sleek appearance and functionality for which Apple would become known. Based on the success of its initial product offerings, the company went public in 1980, resulting in a $1.79 billion valuation that made 300 investors millionaires overnight.[111] Apple's ability—and, more specifically, Jobs' acumen—to use a supplier to finance its product launch, negotiate better prices for the components, and bring investors into the company signified the success that would come decades later for Apple's supply chain management.

The rise to industry leader in supply chain management came only after serious financial losses, the ouster of Steve Jobs, and multiple CEOs. Between 1993 and 1996, Apple removed three CEOs: John Sculley, Michael Spindler, and Gil Amelio.[112] In June 1993, John Sculley was forced out as CEO for a number of perceived missteps: not licensing Apple software to third-party companies, refusing to reconsider product pricing concerns, and supporting the failed Newton Message Pad.[113] Michael Spindler, who rose through the ranks of Apple Europe, was blamed for the failure of Apple's Newton and Copland operating systems.[114] He was also believed to have initiated takeover talks with IBM, Harris, and Phillips before being removed in 1996.[115] During his tenure as CEO, Gil Amelio sought to eliminate low-quality and underperforming product lines. However, Apple's stock hit a twelve-year low at this time, resulting in his ultimate removal.

Beyond Apple's leadership challenges, there were other aggravating factors that contributed to its instability. It was during this period that Microsoft introduced Windows

---

[110] Issacson, *Steve Jobs*, chapter 6.

[111] Ibid.

[112] "Long Bio 8/12," All about Steve Jobs, July 27, 2017, http://allaboutstevejobs.com/bio/longbio/longbio_08.php.

[113] "John Sculley," Biography.com, accessed September 3, 2017, https://www.biography.com/people/john-sculley-21187457

[114] Savitz, "Managing the Risks of a Globalized Supply Chain."

[115] Matt Brian, "A Look at Apple's CEOs from 1977 to 2011," The Next Web, August 24, 2011, https://thenextweb.com/apple/2011/08/25/a-look-at-apples-ceos-from-1977-to-2011/.

95, which was seen as one of the most successful graphical user interface launches ever.[116] In addition, Apple began licensing out its Mac operating system to third-party vendors to install on cheaper products and clones.[117] All of these factors resulted in a significant loss of market share for Apple and a continued downslide in its valuation, which led to the return of the previously ousted Steve Jobs. One of Jobs' first actions to bring Apple back from the brink of failure and make it the industry leader in supply chain management was to eliminate all non-essential product lines. This choice continued ousted CEO Aemlio's work, which had reduced Apple's 350 projects to fifty. Ultimately, Jobs cut the number of Apple projects down to ten.[118]

Jobs' next, and most significant, action was to bring Tim Cook, former vice president of materials at Compaq Computer Corporation, to Apple as the chief operating officer. Cook immediately reduced the number of suppliers from 100 to twenty-four, shrunk inventory turnover from months to days, and cut production time for Apple computers in half.[119] To achieve these milestones, Cook viewed the total product lifecycle through the framework of supply chain management. As a result of these efforts, Apple now defines the standard for supply chain management across disciplines, to include the defense industry.

B. NEW PRODUCT DEVELOPMENT

One of the hallmarks of Apple's success has been the number of innovative and successful products it provides to consumers and the world. The phenomenon began with the company's first offerings, the Apple I and II, which made personal computers accessible to the average household. These initial efforts were followed by the Macintosh, which allowed Apple to accomplish a task that industry leader IBM had been unable to: bring the personal computer to the masses. Apple built on these initial

---

[116] Peter Suciu, "20 Years Later, Windows 95 Launch Brings Tears of Nostalgia and Hilarity," Tech News World, Aug 24, 2015, http://www.technewsworld.com/story/82413.html.

[117] Ken Mark, *Apple Inc.: Managing A Global Supply Chain* (Ontario, Canada: Ivey Publishing).

[118] Tom Hormby, "Think Different: The Ad Campaign that Restored Apple's Reputation," Low End Mac, August 10, 2013, http://lowendmac.com/2013/think-different-ad-campaign-restored-apples-reputation/.

[119] Simpson, "Tim Cook."

successes by introducing other industry-leading products such as the PowerBook, the iMac, and Mac operating systems 7 and 8.

In the early 2000s, Apple changed not only the tech sector but also the personal entertainment and cell phone industries with the introduction of the iPod, iPhone, and iPad. To complement these systems, Apple introduced its iTunes store, where consumers could purchase all the music and media they wanted for their devices. Apple's app store followed soon after, further enabling consumers to acquire media and applications to enhance their existing Apple products. In doing so, Apple created a closed ecosystem in which individuals could purchase devices and all their content from one source. As it grew, Apple continued to develop new products across all departments to create an efficient, seamless process.

For Apple, new product development is not an isolated process contained within the domain of research and development (R&D); the company uses a holistic approach that involves manufacturing, purchasing, logistics, and suppliers. In furtherance of this interwoven effort, Apple has continually increased its R&D spending during the last seven years.[120] For designers and engineers, this approach can translate into months away from home, living out of hotels and working with suppliers and manufacturers as a design idea evolves from the initial concept into a consumer-ready product.[121] In addition to product design and development, Apple engineers coordinate with partner companies to redesign that manufacturing and tooling equipment used to produce Apple products. All of these efforts allow Apple to create a closed ecosystem in which it maintains control of its product development from start to finish without having to outsource components, as done by competitors like Samsung. This near-totalitarian level of control Apple exerts over its supply chain also reduces the potential for the introduction of counterfeit components into its products.

---

[120] Kif Leswing, "Apple Is Spending Billions on Secret R&D Projects—And it Keeps Spending More," *Business Insider*, February 1, 2017, http://www.businessinsider.com/apple-rd-spend-charts-2017-2.

[121] Adam Satariano and Peter Burrows, "Apple's Supply Chain Secret? Hoard Lasers," *Bloomberg Businessweek*, November 3, 2011, https://www.bloomberg.com/news/articles/2011-11-03/apples-supply-chain-secret-hoard-lasers.

An example of how Apple's product development is integrated into the supply chain process is illustrated through the story of the MacBook's little green indicator light. During the redesign of the MacBook circa 2005, lead designer Johny Ives came up with the idea to include a small green light above the screen to identify when the camera was in use. However, to add this simple feature, Ives had to fabricate a means for the light to shine through the product's metal casing. As part of the effort to add this seemingly minor detail, Ives collaborated with a team of manufacturing engineers and material design experts. The team ultimately came up with a process for drilling microscopic holes in the metal frame using a highly specialized laser, thus allowing the indicator light to become visible to the naked eye.[122]

While Ives and the team had developed an effective solution for a single MacBook, they still had to resolve the issue of mass production. To do so, Apple acquiring a massive number of lasers to ensure it could scale up the solution and meet consumer demand in a timely fashion. The design team located a company in the United States that produced the type of lasers needed to move the solution to mass production. While the lasers were originally designed for microchip manufacturing, Apple's engineers were able to make the necessary modifications to produce the desired microscopic holes in the MacBook.[123] As a result, the little green indicator light has become a standard feature on the MacBook Air, Trackpads, and wireless keyboards.[124]

By converting a laser designed for microchip manufacturing into a solution for the MacBook's indicator light, Apple kept production of the product in house. This resulted in Apple persuading the manufacturer to sign an exclusivity agreement for the lasers, which sell for approximately $250,000 each.[125] This is a just one example of Apple's ability to maintain its supply chain and avoid outsourcing to third-party suppliers, as

---

[122] Satariano and Burrows, "Apple's Supply Chain Secret."

[123] Florin, "Samsung Sees Advantages in Outsourcing Smartphone Production. 10 Million Galaxy Trend Duos Units already Made," Unwired View, November 13, 2013, http://www.unwiredview.com/2013/11/13/samsung-sees-advantages-in-outsourcing-smartphone-production-10-million-galaxy-trend-duos-units-already-made/.

[124] Satariano and Burrows, "Apple's Supply Chain Secret."

[125] Ibid.

competitors like Samsung do.[126] This type of design agility, exemplified by Ives, has allowed Apple to maintain "a closed ecosystem where it exerts control over nearly every piece of the supply chain" from the initial concept to the point of sale.[127] These efforts, coupled with the company's massive product volume, availability of significant capital, and ability to negotiate substantial discounts with suppliers give Apple an unparalleled operational edge. As quoted in *Bloomberg Businessweek*, Mike Fawkes, Hewlett-Packard's former supply chain chief, marvels, "Operations expertise is as big an asset for Apple as product innovation or marketing. … They've taken operational excellence to a level never seen before."[128]

C. PROCUREMENT

According to Apple's website, the company's goal is to "obtain stellar products and services within tight timeframes, at a cost that represents the best possible value to … customers and shareholders."[129] Apple uses various means to translate this goal into a practice. First is Apple's storied ability to use its almost unlimited purchasing power to buy all of the existing production capacity or raw materials. This was exemplified when Apple bought up all available high-end drills to produce the iPad 2, which resulted in an increase of competitor wait times for the equipment from six weeks to six months.[130] In another instance, Apple prevented computer manufacturing company HTC from acquiring high-resolution screens for their phones by purchasing all available capacity as part of the iPhone 4 rollout.[131] Apple also employs highly structured long-term contracts with its suppliers. These contracts provide Apple with necessary access to production capacity and materials, which means the company does not have to maintain inventories

---

[126] Satariano and Burrows, "Apple's Supply Chain Secret."

[127] Ibid.

[128] Ibid.

[129] "Apple and Procurement," accessed December 12, 2017, https://www.apple.com/procurement/.

[130] Satariano and Burrows, "Apple's Supply Chain Secret."

[131] See, for example, Josh Ong, "Apple Leverages Deep Pocks to Gain Supply Chain Edge over Rivals," Apple Insider, November 3, 2011, http://appleinsider.com/articles/11/11/04/apple_leverages_deep_pockets_to_gain_supply_chain_edge_over_rivals_report.

or manufacturing capabilities itself. Apple's contracting methodology contrasts starkly with the DOD's process, in which cost concerns frequently override a desire for quality.

Although Apple's practice of buying up all available inventory and capacity can be beneficial to both the supplier and to Apple, it has also proven costly for some suppliers. There have been occasions when Apple's choice to use another supplier or to terminate an existing contract has resulted in significant financial losses for the affected supplier. While most consumers know that Apple and Samsung are rivals, few realize that Samsung is one of Apple's largest suppliers, and therefore, significantly affected by these kinds of deals. Samsung experienced such a loss in 2012 when Apple placed an order for dynamic random access memory chips with Samsung's competitor Elpida.[132] According to a news report, Apple's order was for 50 percent of the total available chips produced by Elpida's Hiroshima plant.[133] The purchase caused Samsung's stock to drop 6 percent in a single day and reduced its market capitalization by $10 billion.

Another consequence for suppliers considering a partnership with Apple is the restrictive long-term contractual obligations that follow the significant upfront capital it offers. In one case, an executive of a major manufacturing firm indicated that the firm turned down a $1 billion upfront payment out of fear of becoming too dependent on Apple and ultimately deflating prices.[134] This fear was fully realized by the British firm Imagination Technologies, which derives more than half of its annual revenue from Apple, when its stock dropped 72 percent following the news that Apple would stop licensing Imagination Technologies' intellectual property, which is used in iPhones, iPads, and Apple watches.[135]

Further evidence of Apple's restrictive contractual obligations are seen in chapter 11 bankruptcy filings from GT Advanced Technologies, which disclosed Apple's

---

[132] "Samsung Market Value Drops $10 Billion On Apple News," WebProNews, May 16, 2012, http://www.webpronews.com/samsung-market-value-drops-10-billion-on-apple-news-2012-05/.

[133] Ibid.

[134] Ong, "Apple Leverages Deep Pockets."

[135] Alanna Petroff, "Apple Dropsa Supplier and its Stock Falls 72%," CNN, http://money.cnn.com/2017/04/03/investing/apple-imagination-technologies-stock/index.html.

usually secretive contract terms. Within this brief overview, the restrictive and one-sided contract terms are clearly evident:

- GTAT was prohibited, for years to come, from conducting any sapphire business with any conceivable Apple competitor or any direct and indirect Apple competitor.
- If GTAT discloses any aspect of the agreements with Apple, it is liable for breach of confidentiality to Apple for ***$50 million per occurrence*** as liquidated damages; Apple, on the other hand, is not liable for any liquidated damages if it violates confidentiality.
- GTAT must accept and fulfill any purchase order placed by Apple on the date selected by Apple. If there is any delay, GTAT, must either use expedited shipping (***at its own cost***) or purchase substitute goods (***at its own cost***). If GTAT's delivery is late, GTAT must pay $320,000 per boule of sapphire (and $77 per millimeter of sapphire material) as liquidated damages to Apple.
- Apple, however, has the right, ***without compensating GTAT***, to cancel a purchase order in whole or in part at any time and reschedule a delivery date at any time.
- GTAT must pay $640,000 per boule that it sells to a third party in violation of the exclusivity restrictions in the contract. Apple had no obligation to buy boules from GTAT.[136]

Additional contract terms are available in the appendix.

While partnering with Apple offers substantial benefits—including industry recognition, a significant revenue stream, and a potential long-term relationship—there are obvious consequences. The downsides can include the aforementioned contract terms, a loss of capital, and the fear of becoming too dependent on Apple as a revenue source. Since Apple exerts the leverage in these relationships, the supplier needs to remain agile and willing to meet Apple's expectations. Two such suppliers include Samsung and Analog Devices Incorporated (ADI). Even though Samsung suffered the previously identified loss, its relationship with Apple has continued, and generates $8 billion

[136] GT Advanced Technologies Inc. v Apple, 14-196116-HJB (CD Delaware, 2014), https://www.kccllc.net/gtat/document/14119161411070000000000003.

annually.[137] ADI is a U.S.-based technology firm that provides Apple with the capacitive touch-screen controllers for iPhones and watches. Purportedly, ADI will provide Apple the much-anticipated 3D controllers for touch screens, which is expected to result in a one-day 10 percent increase in ADI's stock price.[138] When considering partnering with Apple, suppliers must remember that there are hundreds of other companies willing to meet Apple's expectations and demands.

D. PRODUCT ASSEMBLY

In furtherance of the closed ecosystem concept, Apple maintains control of product assembly by continuing to collaborate with its subcontractors. This approach contrasts Apple's competitors, such as Samsung and Nokia, which have opted to outsource their product assembly. Although the terms *subcontracting* and *outsourcing* are often used interchangeably, there is a substantial difference between the two practices. Subcontracting involves hiring another company to execute a specific business function, usually one that cannot be performed internally, with the two parties working collaboratively during the agreement and the hiring party retaining significant control over the process. Conversely, outsourcing refers to a function that could be performed internally, but it is more cost efficient to contract an outside third party to manage the function.[139] Most importantly, the outsourced third-party provider performs the task with little to no oversight from the hiring firm, which only provides feedback as needed. By eliminating the need to outsource production, Apple again reduces the possibility of counterfeit components entering its supply chain.

The close-working relationships between Apple and its partners facilitate agile manufacturing that can meet the needs of changing product designs and consumer

---

[137] Greg McFarlane, "How Apple and Samsung Compare … And Coexist," Investopedia, accessed December 12, 2017, http://www.investopedia.com/articles/markets/102714/how-apple-and-samsung-compare-and-coexist.asp.

[138] Shobhit Seth, "10 Major Companies Tied to the Apple Supply Chain (AAPL)," Investopedia, September 2, 2015, http://www.investopedia.com/articles/investing/090315/10-major-companies-tied-apple-supply-chain.asp.

[139] "What's the Difference between outsourcing and Subcontracting?," Investopedia, March 24, 2015, http://www.investopedia.com/ask/answers/032415/whats-difference-between-outsourcing-and-subcontracting.asp.

demands. Of Apple's partners, Hon Hai Precision Industry Company, more commonly known as Foxconn, is the biggest contributor in terms of product assembly. Founded in 1974, Foxconn is a Taiwanese-based electronics manufacturing firm that employs more than one million people and that, in 2016, bought a majority stake in Japan's Sharp Corporation for $3.5 billion.[140] One of the most storied examples of Foxconn's production agility is the "biscuit and tea story," as told by an Apple executive. The unnamed executive was addressing how an eleventh-hour change necessitated a complete production overhaul, resulting in the following action: "A foreman immediately roused 8,000 workers inside the company's dormitories. Each employee was given a biscuit and a cup of tea, guided to a workstation, and within half an hour, started a 12-hour shift fitting glass screens into beveled frames. Within 96 hours, the plant was producing over 10,000 iPhones a day."[141] Apple executives reportedly admitted that this type of efficiency could not be achieved in the United States.[142]

However, this level of agility and efficiency did not come without its own set of problems. Apple is continually criticized for employing Foxconn to make products that could be made in the United States. However, Apple executive believe that this approach is more cost effective, and that the foreign workers' scalability, agility, and capability have outpaced their U.S. counterparts.[143] Apple has also faced criticism that Foxconn facilities are organized sweatshops. Media outlets and human rights organizations seized upon the number of suicides committed by Foxconn's employees, fourteen in 2010, as the clear indices of Apple's culpability in promoting deplorable working conditions. While the working conditions were abhorrent, and in some cases borderline inhumane, these incidents served as the impetus for Apple to take the lead in corporate social responsibility for its workers around the globe.

---

[140] Kevin Chan, "Foxconn: World's No. 1 Contract Electronics Maker," Phys.org, July 27, 2017, https://phys.org/news/2017-07-foxconn-world-electronics-maker.html.

[141] Duhigg and Bradsher, "iPhone Work."

[142] Ibid.

[143] Ibid.

Since 2011, following the deaths at Foxconn and Tim Cook's establishment as CEO, Apple has considerably increased corporate social responsibility efforts. One such effort was the implementation of Apple's "Supplier Code of Conduct," to which all suppliers must agree and which is considered the toughest in the electronics industry. The code of conduct specifically addresses "labor and human rights, health and safety, environmental protections, ethics, and management practices."[144] The code also provides a level of transparency through which consumers can verify the provenance of the products they are purchasing. This same level of transparency and concern for a product's provenance should be employed throughout the defense industry. To ensure compliance with the code of conduct, Apple conducts audits of all its suppliers' factories. Highlights of the 2017 audits include a 98-percent compliance rate for the 60-hour work week, $2.6 million reimbursed to employees for overcharged recruitment fees, and a number-one ranking for a third year by the Corporate Information Transparency Index.[145] Outside of these efforts, Foxconn is now in negotiations to build its first major American factory in Wisconsin, which will reportedly create at least 3,000 jobs and represent a $10 billion investment.[146]

E. LOGISTICS

The logistics of Apple's supply chain efforts are only realized when an iPhone, iPad, or other product ships from a factory in China and successfully arrives in the hands of consumers, whether in Tokyo, Toledo, or Toronto. While this might be viewed as the last step of the process, it takes months of advance planning, to include sales forecasting, product manufacturing, airfreight acquisition, positioning of inventory around the world, and customer data flow management. For Apple to accomplish these steps, it must display the same agility demonstrated in all other aspects of its supply chain. One of the

---

144 "Apple Supplier Code of Conduct," January 1, 2017, 1, https://images.apple.com/supplier-responsibility/pdf/Apple-Supplier-Code-of-Conduct-January.pdf.

145 "Supplier Responsibility: 2017 Progress Report," Apple, March 2017, https://www.apple.com/supplier-responsibility/.

146 Nelson D. Schwartz and Vindu Goel, "Foxconn Says it Plans to Build a Factory in Wisconsin, Adding 3,000 Jobs," *New York Times*, July 26, 2017, https://www.nytimes.com/2017/07/26/business/foxconn-factory-wisconsin-jobs.html.

early examples of Apple's agility in this area was when then-CEO Tim Cook booked "$100 million worth of holiday season air freight months in advance—ensuring new iMacs were shipped expediently" to arrive in time for the increased holiday demand.[147] Cook's innovative use of air freight occurred at a time when most electronics manufacturers used ocean transport for cost savings, and his decision to do so ultimately left competitors at a loss when they were unable to book air freight. Another example of its evolving agility was when Apple came to the realization, in 2001, that it was cheaper to ship iPods directly to consumers via UPS and FedEx, than to sell them from a retail outlet.[148] In seizing these early opportunities to enhance its logistics operations, Apple portended the dominance it would ultimately exert across the industry.

Building on these early successes, Apple developed an all-encompassing logistical enterprise that seamlessly rolls out millions of products worldwide. The first step in the process is to ensure suppliers have sufficient inventory prior to ramping up production. The next step is assembling all of the relevant data to develop the most accurate sales forecast; failing to do so may result in an insufficient inventory or overruns, potentially costing millions of dollars. Such an economic loss was most recently seen when Microsoft had to write down its net income by $900 million due to a surplus of unsold surface tablets.[149] Following the forecasting, millions of iPhones are produced and shipped to staging points around the globe, accompanied by security personnel. In years past, Apple shipped products in old tomato cartons as a security precaution.[150] Following a product unveiling, the iPhones are moved from the staging points to retail outlets, direct to consumers, and all of this is constantly monitored by Apple to adjust for changes in demands and inventory.[151] Following the initial period, an

---

[147] Simpson, "Tim Cook."

[148] Satariano and Burrows, "Apple's Supply Chain Secret."

[149] Adam Satariano, "The IPhone's Secret Flights from China to Your Local Apple Store," *Bloomberg*, September 11, 2013, https://www.bloomberg.com/news/2013-09-11/the-iphone-s-secret-flights-from-china-to-your-local-apple-store.html.

[150] Matt Rosoff, "Apple once Shipped a Product in Unmarked Tomato Boxes to Prevent Spying," November 2, 2011, *Business Insider*, http://www.businessinsider.com/apple-once-shipped-a-product-in-unmarked-tomato-boxes-to-prevent-spying-2011-11.

[151] Ibid.

after-action breakdown is conducted to address any potential mistakes and improve the process for the next rollout. Through these innovative yet simple methods, Apple continuously ensures the security of its supply chain.

F. CONCLUSION

This chapter highlighted how Apple's supply chain management practices have created a closed ecosystem, which Apple controls from start to finish. Doing so allows Apple to keep its manufacturing in-house, unlike competitors Samsung and Nokia, which have outsourced production. This also allows for agile manufacturing that can meet changing product designs and consumer demands at a moment's notice, alleviating the need for large inventories or product overruns. Apple maintains this closed ecosystem by viewing supply chain management as a holistic process interwoven through all of its components, including manufacturing, purchasing, logistics, and suppliers, instead of utilizing an isolated application under the purview of a single department. In furtherance of this perspective, Apple will use its almost unlimited upfront capital to buy out production capacity, raw materials, or available air freight when manufacturing and rolling out products, thus increasing lag times for competitors. Ultimately, all these protocols minimize the potential for counterfeit components to enter Apple's supply chain. The next chapter takes a look at another example of supply chain management: the United Kingdom's MoD. The chapter reviews the MoD's structure, policies, and procedures to determine how it is achieving success.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. UNITED KINGDOM MINISTRY OF DEFENCE

In response to the Senate Armed Services Committee investigation, other countries began to ask if their defense supply chains had been compromised by counterfeit electronic components. On June 12, 2012, the issue was raised on the floor of the UK Parliament by Lord Maginnis of Drumglass. He demanded to know of Her Majesty's Government "whether any similar components are incorporated in aircraft or military equipment manufactured in the United Kingdom" and "whether they intend to carry out or initiate any similar inquiry in the United Kingdom."[152] The Parliamentary Under-Secretary of State for the Ministry of Defence, Lord Astor of Hever, unequivocally responded with, "The Ministry of Defence Quality Assurance Authority has not received any reports of counterfeit electronic parts having been detected in MoD equipment in the past five years."[153] As a result, it was determined that Parliament would not conduct a similar inquiry; however, due to the significance of the problem, Parliament agreed to establish a Counterfeit Awareness Working Group.[154] To identify how the MoD's supply chain was not inundated with counterfeits—in fact, it had not even a single counterfeit part in five years—this chapter reviews its structure, procurement practices, collaborative approach, and policy guidance.

A. OVERVIEW

In the context of defense acquisition organizations, the United Kingdom's MoD falls into the broader category of a centralized government organization. Under this concept, one organization is responsible for the acquisition of weapons systems and military equipment required by all the components of its armed forces.[155] Within the MoD, the sole agency responsible for all procurement and acquisition activities is known

---

[152] "Armed Forces: Aircraft," UK Parliament Daily Hansard, Column WA237, June 12, 2012, https://www.publications.parliament.uk/pa/ld201213/ldhansrd/text/120612w0001.htm.

[153] Ibid.

[154] "Department for Work and Pensions: Forums," UK Parliament Daily Hansard, Column WA238, June 12, 2012, https://www.publications.parliament.uk/pa/ld201213/ldhansrd/text/120612w0001.htm.

[155] Auger, *Defense Procurement Organizations.*

as Defence Equipment and Support. The agency was formed in 2007 through the merger of two former MoD organizations: the Defence Procurement Agency and the Defence Logistics Organization.[156] On its website, Defence Equipment and Support defines itself as a "bespoke trading entity, and arm's length body of the Ministry of Defence."[157] Defence Equipment and Support has a workforce of approximately 12,000 civil servants and military personnel and in the 2015/2016 fiscal year it spent nearly £19 billion, giving it the fifth largest defense budget in the world.[158]

With Defence Equipment and Support having the sole authority for all procurement and acquisition activities across all UK military components, its hierarchal structure is significant to its success. The organization is led by a CEO. Since 2015, Defence Equipment and Support has been led by Tony Douglas, who was appointed by the prime minister in consultation with the deputy prime minister and defence secretary.[159] Previous to his appointment with the MoD, Douglas worked in the private sector, where he had most recently been the executive director of the Dubai Airport. Under the CEO, there are four three-star posts—chief of materiel (fleet), a Royal Navy vice admiral; chief of materiel (land), a British Army lieutenant general; chief of materiel (air), a Royal Air Force air marshal; and chief of materiel (joint enablers).[160] Through this hierarchal structure, all branches of the British Armed Forces are afforded equal representation in the acquisition and procurement process. This further allows Defence Equipment and Support the opportunity to develop unified weapons platforms and equipment across the different service components, which means they do not need to purchase individualized systems for each component.

---

156 Auger, *Defense Procurement Organizations*.

157 "Defence Equipment & Support," GOV.UK, accessed October 9, 2017, https://www.gov.uk/government/organisations/defence-equipment-and-support/about#corporate-information.

158 "Ministry of Defence," GOV.UK, accessed October 9, 2017, https://www.gov.uk/government/organisations/ministry-of-defence/about/procurement

159 "MOD Announces Appointment of the Chief Executive for Defence Equipment and Support," GOV.UK, March 25, 2015, https://www.gov.uk/government/news/mod-announces-appointment-of-the-chief-executive-for-defence-equipment-and-support.

160 "DE&S Organisation Chart," GOV.UK, May 2017, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/529365/20160527-DESOrgChart.pdf.

B. PROCUREMENT

To further its mission and objectives, Defence Equipment and Support utilizes the Smart Acquisition initiative, which implements a through-life approach to procurement rather than focusing resources primarily on the initial purchase.[161]

The goal of Smart Acquisition is "to acquire defense capability faster, cheaper, better and more effectively integrated."[162] To effectively accomplish this goal, MoD has identified four objectives. The first is to deliver and sustain the capabilities that are outlined at the time major decisions are made, also referred to as "Main Gate" in MoD acquisition terminology.[163] This translates into the ability to deliver and provide the agreed-upon services and support within the context of the contract, without going over budget or beyond the identified milestones. The second objective is to integrate defense capabilities into their respective environments, while still being flexible and adaptable to the changing environments.[164] The goal of this objective is to avoid being locked into standards or technology that was available at the time of a product's development, which in some cases occurred ten to fifteen years previously. The third objective is to acquire defense capabilities progressively and at lower risk. This requires planners to balance military effectiveness, time, and cost in order to provide greater value for the investment, sustain the defense industry, and build effective long-term relationships with suppliers.[165] The fourth and final objective is to reduce the time between development of new systems and their front-line introduction, which could provide distinct military advantages. When this objective is realized, wait times are reduced throughout the acquisition process, for both the development of new technology its approval.[166]

---

[161] Gray, "Review of Acquisition."

[162] UK Ministry of Defence Procurement Agency, "Smart Acquisition Program," U.S. Embassy & Consulate in the United Kingdom, accessed June 25, 2017, https://uk.usembassy.gov/wp-content/uploads/sites/16/2015/08/odc_london_uk_smart_acquisition_program.pdf

[163] *The Acquisition Handbook*, Edition 4 (Bardwell, England: Tactica Solutions, 2002), http://www.defence.org.cn/aspnet/vip-usa/uploadfiles/2004102932134509.pdf.

[164] Ibid.

[165] Ken Hambleton et al., *Conquering Complexity Lessons for Defence Systems Acquisition* (London: The Defence Engineering Group, 2005).

[166] Ibid.

Thanks to Smart Acquisition, Defence Equipment and Support "no longer replaces military equipment, services, or business information systems on a like-for-like basis, but instead takes into account how such capability will integrate with other capabilities to achieve optimum effect for the armed services."[167] As part of the through-life approach, "availability contracts" have replaced traditional support contracts. Similar to the United States, a significant portion of the United Kingdom's budget is spent on defense contracts. However, the United Kingdom uses a contracting for availability methodology, which shifts a significant portion of responsibility from the MoD to the defense contractor. To do so, the MoD shifted from a traditional paradigm, in which the majority of the capital investment went to front-loaded development expenses, to a complete project support model, in which capital investments are distributed across a project's entire lifecycle. This means that contractors retain a greater share of responsibility for support and replacement activities, while the MoD provides resources (e.g., manpower and infrastructure) as part of an integrated support model.[168]

The contracting for availability concept allowed a structural change; the MoD was able to partner with industry, creating a shared-risk model, and thus providing an impetus for industry to meet deadlines.[169] These changes are exemplified in the flowchart in Figure 2.[170]

---

[167] Gansler, Lucyshyn, and Harrington, "Through Life Support Capability Management," 14.

[168] Gray, "Review of Acquisition."

[169] Ibid.

[170] National Audit Office, *Transforming Logistics Support for Fast Jets* (London: The Stationery Office, 2017), https://www.nao.org.uk/wp-content/uploads/2007/07/0607825.pdf.

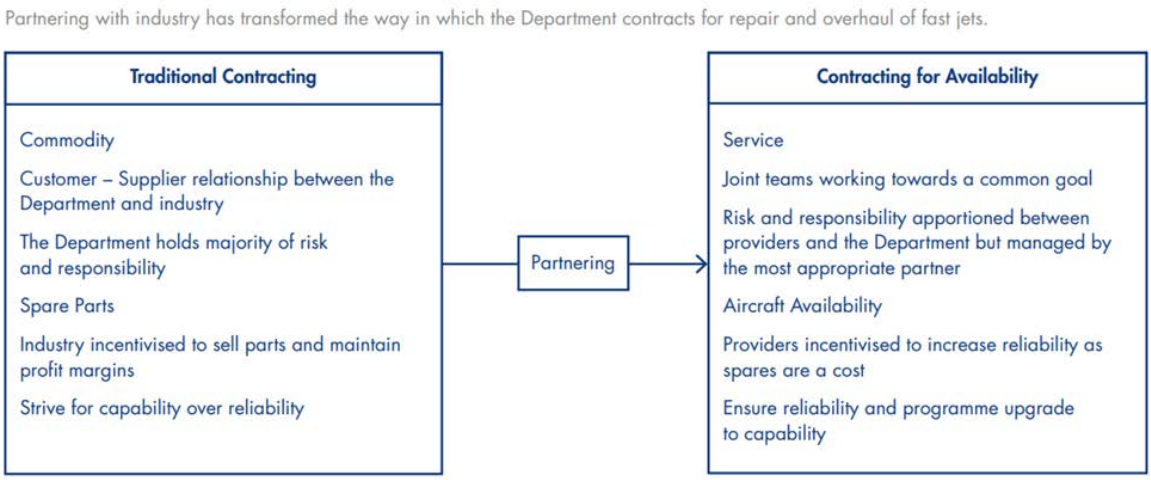
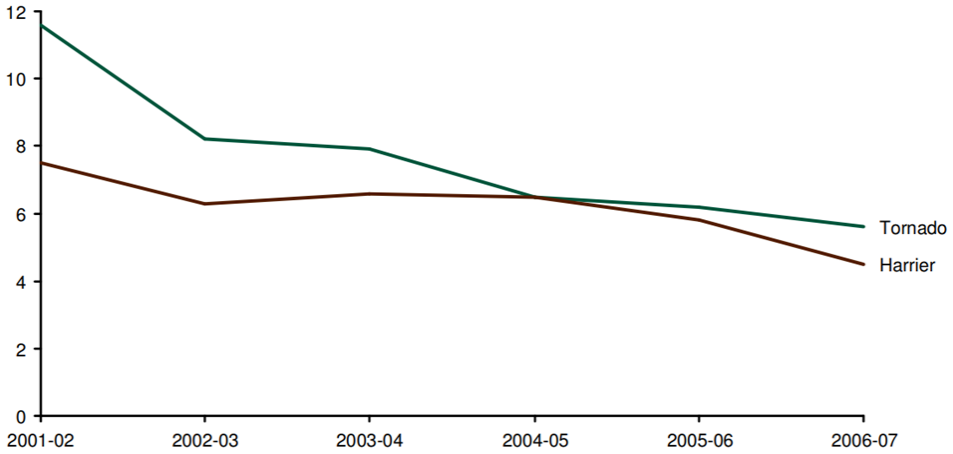


Figure 2. MoD Contracting for Availability: Partnering with Industry[171]

Figure 3 provides an example of the significant cost savings that were achieved by the contracting for availability model when implemented for the procurement of the MoD's Tornado and Harrier aircraft.[172]



Thousands of pounds.

Figure 3. Cost per Flying Hour for Tornado and Harrier Aircraft[173]

[171] Source: National Audit Office, *Transforming Logistics Support*, 26.

[172] Gray, "Review of Acquisition."

[173] Source: Gray, "Review of Acquisition."

Lastly, before availability contracts are implemented, they are reviewed by program boards to ensure they are value-enhancing projects.[174]

The Smart Acquisition methods, which include the through-life concept and the contracting for availability process, have produced significant cost savings for the MoD. They have also redistributed responsibilities between the MoD and the defense contractors, resulting in two additional benefits. First is the increased level of responsibility assigned to the contractor, which incentivizes the contractor to meet established timelines and budgetary milestones. Second, and maybe more importantly, the Smart Acquisition methods have enhanced the relationships between the United Kingdom's defense industry and the MoD. These relationships also foster other collaborative efforts between the MoD, industry members, and subject-matter experts.

C. POLICY GUIDANCE

The MoD has also sought to ensure supply chain security by implementing policy that industry personnel can use to assess their supply chains. In this vein, Defence Standard 05-135, Issue 1: *Avoidance of Counterfeit Material*, was issued on July 10, 2014. The standard was developed by the MoD in collaboration with the UK defense community and industry experts. The standard uses a risk-based model that provides contractors with a means to evaluate the authenticity of their materials and to develop a greater awareness of their supply chains. According to the MoD, "This Defence Standard defines the arrangements that a supplier is required to establish to demonstrate that they are actively planning and managing the risk of counterfeit materiel in their supply chain to prevent delivery of such materiel to the MoD."[175] Once again, this places a greater onus on the defense industry to identify and manage the risk within its supply chains. The supplier must verify that materials destined for the supply chain meet identified performance standards and safety requirements and that the material is not diminished.

While the standard provides industry with an established guideline to manage the risk in its supply chains, it ultimately serves to prevent counterfeit materials from

[174] Gray, "Review of Acquisition."

[175] Ministry of Defense, *Avoidance of Counterfeit Materiel*, DEF STAN 05-135, iii.

entering the defense supply chain. The prevention efforts are achieved through four different approaches. The first two initiatives—to increase awareness throughout the defense industry, and to share best practices, go hand in hand.[176] To accomplish these initiatives, the MoD works collaboratively with its industry partners to share best practices at industry events, to include the MoD counterfeit awareness event. In addition, all best practices and counterfeit awareness material are posted on the MoD's Acquisition System Guidance website.[177] This site can be accessed by all MoD and industry personnel. The next step in the prevention model is the use of a standardized, risk-based approach.[178] While this risk-based approach does not mandate a standard to be utilized, it does require the supplier to demonstrate the following requirements: a documented policy, training, purchasing, test/verification, control of nonconforming material, and reporting of counterfeit material.[179] The last step in the prevention process is to continually assess opportunities for process improvement. To accomplish this, the MoD periodically reviews all feedback they receive from defense and industry personnel through all of the aforementioned channels, and uses this information to enhance and improve its policies and guidance.

D. COLLABORATIVE APPROACH

As identified on the Defence Equipment and Support website, one of the agency's first priorities is "transforming the organisation so that it can better support the armed forces."[180] Of the varied efforts used to realize this priority, the most impactful is collaboration. BAE Systems articulated the importance of this approach during a 2012 UK MoD Counterfeit Awareness event, when a spokesperson claimed, "Buying from third parties is necessary—complete vertical integration of supply chain in-house to exert

---

176 J. Bullock et al., *Counterfeit Avoidance Maturity Model* (Version1) (Bristol, UK: Ministry of Defense, 2015). https://www.erai.com/CustomUploads/ca/wp/Counterfeit_Avoidance_Maturity_Model.pdf.

177 Ibid.

178 Ibid.

179 Ibid.

180 "Defence Equipment and Support," UK.GOV, accessed October 10, 2017, https://www.gov.uk/government/organisations/defence-equipment-and-support/about.

the most control over sourcing and manufacture is not possible in today's world."[181] Defence Equipment and Support has undertaken a number of initiatives in this effort. The first was the formation of the Counterfeit Awareness Working Group, which was announced by Lord Astor in response to Lord Maginnis' inquiry into the issue of counterfeit components in the UK military. The next initiative was the development of the Counterfeit Avoidance Maturity Model, which serves to provide an appropriate understanding of Defence Standard 05-135.

As part of its collaborative approach, the Counterfeit Awareness Working Group has arranged and sponsored multiple awareness events on counterfeit parts for both MoD and industry personnel. During these events, industry partners have provided a breadth of presentations on topics that include managing supply chain risks, legislative proposals, detection and avoidance of counterfeit parts, and establishment of industry standards. As part of these presentations, industry leaders outlined the efforts being undertaken to ensure their compliance with MoD standards and the efforts used by industry as a whole. One such effort is the creation of the Anti-Counterfeiting Forum, a private industry platform designed to "exchange, develop and disseminate best practices and intelligence to mitigate against the threat of counterfeits in the electronic and electrical supply chains."[182]

To mitigate the threat of counterfeits in the supply chain, the Anti-Counterfeiting Forum uses a multifaceted approach. It starts by building and maintaining close working relationships with representatives from both government and industry entities.[183] In an effort to build these relationships, forum representatives regularly participate in government- and industry-sponsored events. The Forum also hosts an annual counterfeiting awareness seminar. The annual seminar is yet another opportunity for those in the defense community to learn about new developments and industry standards,

---

[181] Mike Falls and Simon Hall, "Thoughts of an OEM on Misrepresented Supply," ESCO, July 7, 2012, https://www.esco.org.uk/download/mod_counterfeit_awareness_event_-_7_july_2016/CAE16_PPT_07-BAE-Systems.pdf.

[182] "About the Anti-Counterfeiting Forum," accessed December 12, 2017, www.anticounterfeiting forum.org.uk/about.aspx.

[183] Ibid.

and to share best practices for managing the risk of counterfeits in the supply chain. The Forum also uses its website to advance its mission. The site provides a wealth of publicly accessible materials that discuss best practices, reference materials, regulatory guidance, and potential solutions providers.[184] The site also contains a page that monitors suspected or alleged counterfeits, though the page is only accessible to registered users.

The Counterfeit Awareness Working Group also develops guidance for the MoD related to counterfeit material and its impact to the defense supply chain. Likely the most substantial piece of guidance issued by the group is the Counterfeit Avoidance Maturity Model, further identified as the "UK MoD Counterfeit Avoidance Working Group support document for auditors assessing compliance with the requirements of Defense Standard 05-135."[185] The Avoidance Model was issued in July 2015, with the goal of providing a consistent interpretation of Defense Standard 05-135 for both MoD and industry personnel.[186] The Model accomplishes its aim by providing supporting guidance that reflects industry-wide best practices.[187] Significantly, this document is a work in progress; the Counterfeit Awareness Working Group plans to further develop the document based on the feedback and experiences of the auditors and assessors who use the model to determine the suitability of suppliers in accordance with Defence Standard 05-135. In fact, the model's annex C, whose purpose is to "assess maturity level," is nothing more than a blank placeholder in the first iteration; the intent is to add practical information and advice in subsequent versions.

E. CONCLUSION

This chapter has demonstrated how the MoD's approach to procurement and acquisition has worked to realign the balance between defence and the industry. Through its innovative use of Smart Acquisition, which includes the through-life concept and contracting for availability, the MoD has redistributed responsibility between defence and

---

[184] Anti-Counterfeiting Forum, accessed December 12, 2017, www.anticounterfeitingforum.org.uk/.

[185] Bullock et al., *Counterfeit Avoidance Maturity Model*.

[186] Ibid.

[187] Ibid.

industry. In so doing, it has incentivized industry to heed milestones and deadlines, resulting in significant savings for the MoD. Additionally, the MoD has taken a much more collaborative approach to working with industry. This is seen through its joint development of Defence Standard 05-135, the Counterfeit Awareness Working Group, and the numerous industry events it has conducted or sponsored. All of this continues to result in a secure supply chain that has not been inundated with counterfeit components or materials.

V. FINDINGS AND CONCLUSIONS

It has been nearly six years since the release of the Senate Armed Services Committee investigation, and the problem of counterfeit components has worsened. The level of sophistication in today's counterfeits has progressed from recycled parts that are refurbished to look new, to newly created parts that were reverse engineered. In light of the continued problem and the growing sophistication of today's counterfeits, the DOD and government at large continue to struggle with how to defend against these counterfeit components. The initial action was a bipartisan response from Congress in the form of an amendment, section 818, to the 2012 National Defense Authorization Act. However, it took another two years before the final rule was passed, implementing section 818. Additionally, there are portions of section 818 that remain undefined and unresolved.

The 2011 Senate Armed Services Committee investigation did not identify a new phenomenon; it simply brought awareness to the problem of counterfeits in the defense supply chain. Counterfeiting has been a practice for more than two millennia; however, based on the sophistication of today's counterfeits, it has taken on an advanced level of significance. The threat posed to the defense supply chain by today's counterfeit electronic components goes beyond a compromised system or piece of equipment. It now threatens our national security and the very lives of those who swore to protect it. The pressing issue, now, is how to defend the defense supply chain.

In researching the methodologies that Apple and the United Kingdom's MoD use to manage their respective supply chains, this thesis identified a number of key concepts. Many of these practices are now identified as industry standards. Accordingly, a broad spectrum of industries use these methodologies to manage their supply chains. These concepts helped establish a set of best practices for supply chain management. This chapter highlights the findings to support these best practices, recommends how they could be incorporated into the defense supply chain, and offers suggestions for future research.

A. FINDINGS

1. Integrated Approach to Supply Chain Management

As supply chains become increasingly globalized, the level of complexity needed to manage them increases. The suppliers, manufacturers, warehouses, and distributors that compose the supply chain span multiple continents and economies. It is thus absolutely essential for supply chain management to encompass every function of the supply chain. As a result, an integrated approach to supply chain management is not only a best practice, but may ultimately be the determinant for success.

a. Apple's Closed Ecosystem

As described in Chapter IV, Apple's approach to supply chain management is completely integrated and holistic. Apple's supply chain management efforts start with new product development and are then interwoven through every aspect of the company to include procurement, manufacturing, and logistics. This approach not only allows Apple to retain greater control over its supply chain, but alleviates the need for outsourcing any of its processes. This methodology also affords the different components within Apple the opportunity to plan for each step of the process, ranging from materials acquisition to delivery of the final Apple product to the consumer. Through this advanced degree of integration, Apple maintains a level of agility attained by few other companies. Accordingly, its integrated methodology for supply chain management is a best practice and has been recognized as the industry standard since 2008 by Gartner, an independent advisory firm.

b. The MoD Smart Acquisition

Through Smart Acquisition concepts, which include through-life support and contracting for availability, the United Kingdom's MoD is moving away from the traditional approach to replacing military equipment on a one-for-one basis, and is instead working to integrate individual resources into broader systems. The Smart Acquisition objectives, articulate this approach by identifying the need to integrate defense capabilities into their respective environments, while maintaining the flexibility

and adaptability needed to navigate changing environments. Ultimately, the Smart Acquisition principles have allowed the MoD to redistribute responsibilities between defence and industry, resulting in a shared-risk model that improve industry's performance and reduces the MoD's costs.

2. Collaboration

During the last decade, *collaboration* has become a buzzword for government and industry alike. When executed properly, collaboration can break down barriers, both internal and external, increase information sharing, and provide greater agility in production and distribution. Both sides of a collaborative relationship can realize all these benefits.

a. Apple's Collaborative Efforts

As it does with its integrated supply chain, Apple employs the collaborative approach throughout its components and processes. This starts with the product development process, during which Apple designers and engineers spend months on the road, working directly with suppliers and manufacturers to ensure a product's evolution. The collaborative process continues between Apple and its subcontractors, which has allowed Apple to retain control of its product manufacturing. The close working relationships between Apple and its subcontractors, such as Foxconn, have resulted in an unsurpassed level of manufacturing agility and efficiency, allowing Apple to respond to any changes in the market. The collaborative process culminates with Apple's logistics process, in which all of its internal components work synergistically to ship, position, and deliver products to customers across the globe.

b. The MoD's Collaborative Efforts

When the MoD established the Counterfeit Awareness Working Group, it both acknowledged the seriousness of the counterfeit issue and adopted a collaborative approach. The Working Group has gone on to hold numerous events to bring awareness to the problem and impress its significance across the industry. These efforts have allowed government and industry to share best practices for identifying and reporting

counterfeit components. Additionally, these efforts fostered the development of the Counterfeit Awareness Forum, a private-industry platform designed to mitigate the threat of counterfeit electronics to the defense supply chain. Defence Standard 05-135 also highlights the MoD's collaborative initiative, providing suppliers with guidelines to assess the risk in their supply chains. The MoD, defense industry, and subject-matter experts jointly developed this standard.

3. Contracting Practices

Successful contracts benefit all parties involved in the acquisition process. To work successfully, contracts must effectively define, communicate, and manage a set of achievable metrics. Failure to establish these essential criteria can result in missed timelines, outdated technologies, and the need to expand the project scope; any of these factors can prove costly to all parties involved.

a. Apple's Contracting Practices

Apple's use of highly structured, long-term contracts has significantly contributed to its success. In these contracts, Apple uses its significant upfront capital to negotiate more favorable terms. In so doing, it provides a source of leverage to ensure its suppliers remain agile and responsive. While this has resulted in companies like GT Advanced technologies filing for chapter 11 bankruptcy protection, it has proven extremely beneficial for others. Two examples include Samsung, which earns billions of dollars annually from its contract with Apple, and Analog Devices Incorporated, which experienced significant stock gains based on the relationship.

b. The MoD's Contracting Practices

As part of its Smart Acquisition concept, the United Kingdom's MoD has exponentially increased its use of contracting for availability. This type of approach required a shift from the traditional customer-client model, in which the majority of capital went into initial product development, to a complete project support model. This new model required the distribution of capital investments across a product's entire lifecycle. Additionally, a greater share of responsibilities for support and replacement

activities are proportioned to the defense contractors. This further resulted in the opportunity for a structural change, allowing the MoD to partner with industry in a shared-risk model, thereby providing industry with the impetus to be more responsive to the needs MoD's needs.

4. Policy

Similar to well-written contracts, policies define and articulate a measurable set of mandatory criteria and guidelines. However, while policies apply to all actors involved in an identified industry or process, contracts are only applicable to the signatories of the contract. In addition to establishing criteria and guidelines, policies serve to develop consistent work processes that are easily repeatable and achievable by all actors. Lastly, when industry data and feedback are used to review established policies, they can serve as the foundation for process improvement.

a. Apple's Supplier Code of Conduct

Apple's Supplier Code of Conduct, which was created after Apple found abhorrent working conditions at a number of its subordinate facilities, is the toughest in the electronics industry. The code was designed to address "labor and human rights, health and safety, environmental protections, ethics, and management system issues."[188] All suppliers and subcontractors must agree to the code's terms and conditions of conduct. Apple annually audits all its suppliers' facilities to ensure compliance with the code of conduct. By requiring this compliance, Apple has established another industry metric.

b. MoD Defence Standard 05-135

With the issuance of Defence Standard 05-135, the MoD sought to prevent counterfeit electronics from entering the defense supply chain. The standard was the result of a collaborative effort between the MoD, the defense community, and industry experts. At the heart of the standard is a risk-based model that affords suppliers with a

[188] Apple, "Apple Supplier Code of Conduct," 1.

means to evaluate their own supply chains. In doing so, the MoD places a greater share of responsibility on the defense industry to identify and manage the risk within its supply chains. Suppliers must verify that materials destined for the defense supply chain are not counterfeit or of diminished capacity.

B. RECOMMENDATIONS

1. Integrated Supply Chain

To combat the issue of counterfeit electronics while providing the advanced technology today's military needs, the DOD's procurement system must adopt a more integrated approach. In May 2017, the House Armed Services Committee was advised by the "809 Panel" that the "Pentagon acquisition system has gotten so bad that it is undermining the nation's military and literally obstructing modernization efforts."[189] In an effort to address the DOD's antiquated methods, the DOD should implement Apple and MoD best practices where possible.

2. Collaboration

The DOD needs to adopt a more collaborative approach with its industry stakeholders and partners at all stages of the procurement process. The DOD's inability to provide contractors with an established standard through which to evaluate their counterfeit parts avoidance and detection systems, as required by section 818 of the 2012 National Defense Authorization Act, exemplifies the lack of collaboration.

3. Contracting Practices

The DOD needs to move to a contracting for availability concept in order to increase the degree of leverage in its contracts, realize increased savings, and place great responsibility on its industry partners. The DOD's current use of performance-based logistics contracts does not facilitate the gains that could be achieved through contracting for availability. In addition, a 2015 report by the Center for Strategic and International

[189] Sandra Erwin, "DOD Wastes Billions on Outdated Technology, 809 Panel Tells HASC," Breaking Defense, May 17, 2017, https://breakingdefense.com/2017/05/dod-wastes-billions-on-outdated-technology-809-panel-tells-hasc/.

Studies reported that the Defense Logistics Agency is missing out on $1 billion in savings due to insufficient use of performance-based logistics contracts.[190]

4. Policy

The DOD needs to more effectively develop and use policy to guide the actions of defense contractors and suppliers. On April 26, 2013, the DOD issued an internal instruction titled "DOD Counterfeit Prevention Policy," which provides guidance for DOD components but does nothing to enlist or guide industry in preventing counterfeit components from entering the defense supply chain.

C. AREAS FOR FUTURE RESEARCH

The purpose of this thesis was to advance DOD efforts to defend the defense supply chain against counterfeit electronic components and the threat they pose to national security. It has made recommendations that the DOD could apply to its acquisition process, policy, or relationships with industry stakeholders. The recommendations are based on methodologies and practices of organizations that have continually demonstrated the ability to successfully manage and defend their supply chains from intrusion by counterfeit components. These recommendations are based on the broader concept of supply chain management, which leaves several other areas for further research.

1. Enforcement Efforts

Around the globe, multiple law enforcement agencies have been combating the epidemic of counterfeit electrical components. These efforts range from individual agencies interdicting counterfeit components to international multiagency operations that seek to target and dismantle organized counterfeiting networks. Two of the early, large-scale international operations, which began in 2005, included Cisco Raider and Network

[190] Scott Maucione, "DLA Falling Short of its Own Policy to Use Performance Based Contracts," Federal News Radio, October 19, 2015, https://federalnewsradio.com/acquisition/2015/10/study-calls-dla-use-performance-based-contracts/.

Raider.[191] These actions specifically targeted "counterfeit network hardware, in particular network routers, switches, network cards and modules manufactured by Cisco," and other well-known companies.[192] As previously mentioned these operations resulted in more than thirty-five search warrants, forty convictions, and the seizure of $220 million in counterfeit network hardware.[193] A more current and ongoing initiative is Operation Chain Reaction. This joint operation, comprising sixteen federal agencies, began in 2011 and specifically targets counterfeit goods entering the DOD supply chain.[194] While these efforts boast significant vanity statistics, there is little research to validate or dispute the operation's ability to effectively combat the problem of counterfeit components.

2. Unique Identifiers

The Defense Logistics Agency is using a recent technological advancement—marking components with plant DNA—to combat counterfeit components. The company responsible for the technology, Applied DNA Sciences, claims the use of this technology guarantees authenticity, as it is impossible to fake.[195] This basis for this claim lies in the proprietary nature of the process, which scrambles the genetic sequencing of the DNA before it is applied to a component.[196] Research into this type of technology may yield a process by which all new components could be marked with a unique identifier that cannot be copied.

---

[191] Department of Justice, "Counterfeit Network Hardware."

[192] Cooney, "Counterfeit Cisco Network Hardware."

[193] Homeland Security Newswire, "China Syndrome: Operation."; Department of Justice, "Counterfeit Network Hardware."

[194] "Operation Chain Reaction Fact Sheet," National Intellectual Property Rights Coordination Center, accessed December 11, 2016, https://www.iprcenter.gov/reports/fact-sheets/operation-chain-reaction-fact-sheet/view.

[195] Tam Harbert, "Plant DNA vs. Counterfeit Chips," *IEEE Spectrum*, May 3, 2012, https://spectrum.ieee.org/semiconductors/devices/plant-dna-vs-counterfeit-chips.

[196] Ibid.

3. Structural Change to DOD Acquisition

Efforts aimed at changing or improving defense acquisition will be significantly hampered by the number of agencies involved in the process. While there have been multiple reports and studies on restructuring the DOD acquisition agencies, dating back to the 1986 Packard Commission, there has been little movement or change. Accordingly, further research focusing on the restructuring of DOD acquisition agencies from twenty-two separate agencies to one central agency needs to be considered.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. GT ADVANCED TECHNOLOGIES CHAPTER 11 BANKRUPTCY FILING

UNITED STATES BANKRUPTCY COURT
DISTRICT OF NEW HAMPSHIRE

In re:	:	**Chapter 11**
GT ADVANCED TECHNOLOGIES INC., *et al.*,	:	**Case No. 14-11916-HJB**
Debtors.[1]	:	**Jointly Administered**

SUPPLEMENTAL DECLARATION OF DANIEL W. SQUILLER IN SUPPORT OF CHAPTER 11 PETITIONS AND FIRST-DAY MOTIONS

I, Daniel W. Squiller, hereby declare under penalty of perjury:

1. I am the Chief Operating Officer of GT Advanced Technologies Inc. ("GT"), a corporation organized under the laws of the State of Delaware with its headquarters located in Merrimack, New Hampshire. GT is the direct and indirect parent of the debtors and debtors in possession in the above-captioned cases (collectively, "GTAT" or the "Debtors") and certain non-debtor affiliates which have not sought chapter 11 relief (together with GTAT, the "GTAT Group"). In that capacity, I am particularly familiar with GTAT's business relationship with Apple, Inc. ("Apple") and GTAT's operations at a facility in Mesa, Arizona (the "Mesa Facility") that is owned by an affiliate of Apple.

2. I have served as Chief Operating Officer since January 14, 2013. Before joining GT, I served as the chief executive officer at PowerGenix, an innovator in high-power battery technology. At PowerGenix, I led the growth of the company to a successful, global high

[1] The debtors in these chapter 11 cases, along with the last four digits of each debtor's tax identification number, as applicable, are: GT Advanced Technologies Inc. (6749), GTAT Corporation (1760), GT Advanced Equipment Holding LLC (8329), GT Equipment Holdings, Inc. (0040), Lindbergh Acquisition Corp. (5073), GT Sapphire Systems Holding LLC (4417), GT Advanced Cz LLC (9815), GT Sapphire Systems Group LLC (5126), and GT Advanced Technologies Limited (1721). The Debtors' corporate headquarters are located at 243 Daniel Webster Highway, Merrimack, NH 03054.

volume manufacturer with its operations in China. Prior to PowerGenix, I was president of the Power Components Division of Invensys, where I managed that Division's global operations. I earned a Bachelor of Science degree in electrical engineering and a Master's degree from Ohio University.

3. On October 6, 2014, I submitted a declaration ("Declaration") in support of GTAT's chapter 11 petitions and certain first day motions. I submit this supplemental declaration ("Supplemental Declaration") to provide further assistance to the Court and other parties in interest in understanding the circumstances that compelled the commencement of these chapter 11 cases and in support of certain additional relief, in the form of motions and applications, that GTAT has requested of the Court (collectively, the "Additional First Day Pleadings").

4. Except as otherwise indicated, all facts set forth in this Supplemental Declaration are based upon my personal knowledge, my discussions with other members of GTAT's senior management and advisors, my review of relevant documents, or my opinion based upon experience, knowledge, and information concerning GTAT's operations and financial affairs. If called upon to testify, I would testify competently to the facts set forth in this Supplemental Declaration. I am authorized to submit this Supplemental Declaration on behalf of GTAT.

SUMMARY OF EVENTS LEADING UP TO CHAPTER 11

5. The GTAT Group has been a diversified technology company producing advanced materials and equipment for the global consumer electronics, power electronics, solar and light-emitting diode ("LED") industries for many years. Among other things, the GTAT Group has more than 40 years of experience developing technological innovations in connection with the manufacturing of furnaces to grow sapphire for industrial use. After diamonds, sapphire is the second hardest substance on Earth. Sapphire is scratch-resistant and has other properties

that make it an ideal material for display applications where those properties provide significant advantages over strengthened glass or other materials used in the consumer electronics field. Sapphire can be fabricated into a variety of shapes and sizes for use in consumer electronics, as well as the military, LED industries, and other industries. In the consumer electronics field, sapphire is currently used in watch crystals, camera lenses, and smartphone displays.

6. As discussed more fully below, this restructuring was necessitated because GTAT's business relationship with Apple has become unsustainable without Apple taking responsibility for cost overruns and additional expenses caused by Apple as described in this Supplemental Declaration. While operating under the October 31, 2013 manufacturing, supply, loan, and related agreements with Apple (collectively, the "Apple Agreements"), GTAT incurred losses—resulting in the current liquidity crisis—due to Apple's inordinate control over GTAT's liquidity, operations (including control over product specifications), and decision making. Although Apple is, ostensibly, a customer of GTAT, Apple strategically structured the transactions with GTAT so that its role would be more akin to that of a lender than a customer. Thus, unlike most customer-supplier relationships, Apple treats the payments it makes for GTAT's products as a "loan" and has taken liens on assets in GTAT's business to secure repayment of those loans. But, beyond this "lender" relationship, Apple embedded itself in the operations of GTAT at the Mesa Facility in a manner that has forced GTAT to divert an inordinate amount of its cash and corporate resources to its operations at the Mesa Facility, and affected GTAT's continued viability as a whole. Apple also embedded itself in GTAT's facility in Salem, Massachusetts (the "Salem Facility") that took on the function of an experimental research and development center for the Apple project. Consequently, GTAT has been unable to use that facility for other revenue streams.

7. GTAT's fabrication costs of the sapphire material grown in the Mesa Facility and Salem Facility furnaces are higher than envisioned, largely because the majority of the fabrication equipment (in contrast to "growth equipment," *i.e.*, the furnaces) selected by Apple for sapphire material could not economically produce a product that Apple would accept. Moreover, GTAT was required to obtain Apple's consent before it could make changes to equipment or processes, and Apple, at least initially, was not willing to permit fabrication equipment changes that would economically produce acceptable product. GTAT was unable to negotiate changes to the pricing regime established by Apple in the transaction documents, and, therefore, GTAT was forced to sell every unit of sapphire material at a substantial loss. GTAT's losses would have increased substantially in 2015 when the price for finished sapphire material is scheduled to decrease under the agreements with Apple. To date, GTAT has incurred approximately $900 million in costs in connection with the Apple project, and, at Apple's dictated pricing, GTAT would never realize a profit.

8. In light of the aggregate effect of all of Apple's actions, as well as Apple's recent pre-petition actions making clear that it was unwilling to negotiate changes to the Apple Agreements necessitated by its own actions and necessary for GTAT to operate profitably, GTAT reluctantly commenced these chapter 11 cases to preserve the value of its business by extracting itself from Apple's control. Among other things, GTAT intends to use the remedies available to it under chapter 11 to reject certain agreements with Apple and expeditiously wind down its Apple-related operations in the Mesa Facility and the Salem Facility. Unfortunately, the winding down of these operations will result in the loss of over 1,300 jobs (including temporary workers). Nevertheless, this step is critical to GTAT's survival as a going concern. Once GTAT has extracted itself from Apple's control, GTAT believes that the completion of its

restructuring efforts will allow it to focus its resources on the operation of its core business of selling sapphire furnaces and other products. Reorganized with an appropriate capital structure, GTAT would emerge from chapter 11 in a stronger position and with a sustainable business model that will allow it to compete effectively in the marketplace.

9. As a result of onerous non-competition provisions in the Apple Agreements, GTAT has been shut out of the global market for its highly valuable sapphire material and equipment. By using the tools available in chapter 11, GTAT believes that it will be able to tap into substantial pent-up demand for sapphire material and equipment in the consumer smartphone and smartwatch markets, segments in which GTAT is currently prohibited from participating.

Background of Relationship with Apple and Apple's "Bait-and-Switch" Strategy

10. With a classic bait-and-switch strategy, Apple presented GTAT with an onerous and massively one-sided deal in the fall of 2013. At the outset of negotiations, Apple had offered GTAT what would have been the company's largest sale ever: an order for 2,600 sapphire growing furnaces. In that scenario, GTAT would operate the furnaces on Apple's behalf, but Apple would own the furnaces. Apple's size and prominence make it the ultimate technology client to land. The deal with Apple was viewed as a potential game-changer for GTAT.

11. In hindsight, it is unclear whether Apple ever intended to purchase any sapphire furnaces from GTAT. Indeed, after months of extensive negotiations over price and related terms, Apple demanded a fundamentally different deal: Apple no longer wanted to buy furnaces from GTAT; instead, Apple offered an arrangement that required GTAT to borrow money from Apple to purchase furnace components and assemble furnaces that would be used to grow

sapphire for Apple. The new structure, as a contract matter, shifted all economic risk to GTAT, because Apple would act as a lender and would have no obligation to purchase any sapphire furnaces, nor did it have any obligation to purchase any sapphire material produced by GTAT. At the same time, Apple constrained GTAT from doing business with any other manufacturer in or supplier to the consumer electronics market, subject to extreme penalties—styled as "liquidated damages"—GTAT failed to meet any of Apple's requirements.

12. Under Apple's new proposal, GTAT was required to acquire 2,036 sapphire furnaces using a prepayment—or "loan"—from Apple of up to $578 million (however, to date Apple has withheld the last $139 million of that "loan"). This structure would enable Apple to purchase sapphire material from GTAT at below market value. This is due to the fact that Apple's "prepayment" was calculated based on ***the cost to GTAT of the furnaces and related equipment*** used to produce sapphire material. GTAT would then manufacture sapphire according to Apple's specifications—which have continually changed and remain in flux to this day—and "repay" the Apple loan using either cash or completed sapphire material as the currency for the repayment.

13. Even if this business transaction worked exactly as contemplated in the original agreements,[2] GTAT would not earn any income at all unless Apple opted to "buy" sapphire material in excess of loan "repayment" obligations. By failing to compensate GTAT for losses associated with the development of the technology due to Apple's constant interference over which GTAT had little or no control, including losses caused by Apple's changes in product specifications, GTAT was forced into the role of a "captive" supplier to Apple, bearing all of the risk and all of the cost, including the costs of more than 1,300 temporary and permanent

---

[2] This assumes that Apple would not have used the fact that it has ***no*** obligation to buy ***any*** sapphire as leverage to impose even more onerous and inequitable terms on GTAT.

personnel, utilities, insurance, repairs, and raw materials. Indeed, the total cost incurred by GTAT pursuant to the project with Apple has so far amounted to approximately **$900 million**. Meanwhile, by the time the Apple project would have been completed seven years later, Apple would have obtained a groundbreaking product from GTAT at below-market cost and GTAT would own 2,036 well-used furnaces with limited resale value.

14. Moreover, if Apple ever decided that it did not want sapphire material, GTAT would be required to repay the full amount of the "loan" in cash. If that eventuality transpired, GTAT would not have hundreds of millions of dollars in cash needed to repay the loan, and Apple could immediately "foreclose" on the 2,036 furnaces and related equipment. Apple sought to secure these obligations through an artificial structure it believed was "bankruptcy remote" and that existed solely to shield Apple from risk. With the very limited exception for pre-existing orders, Apple also prevented GTAT from marketing its furnaces—and thus finding alternative value-maximizing uses for them—through sales to third party purchasers and suppliers to competitors of Apple. Simply put, Apple constructed a risk-free option to acquire millions of highly-engineered units of sapphire material.

15. In October 2013, however, GTAT was out of options because it had invested months negotiating a sale contract with Apple while being effectively locked out of pursuing other opportunities with Apple's competitors. While GTAT had initially marketed its sapphire furnaces to other manufacturers of consumer electronics, those alternative avenues were not further pursued by GTAT given Apple's offer of the most significant contract in the company's history. In any event, the extensive and all-consuming nature of negotiations with Apple would have allowed little time to pursue alternatives. Knowing that GTAT had no practical choice at

that stage other than to concede to Apple's terms, Apple forced a set of agreements on GTAT that, in combination with Apple's economic leverage, put Apple in *de facto* control of GTAT.

Apple Tells GTAT That It Doesn't Negotiate Contracts

16. What ensued was anything but an arm's-length negotiation. Apple simply dictated the terms and conditions of the deal to GTAT. Apple advised that (a) GTAT's management should "not waste their time" trying to negotiate as would normally occur in commercial transactions because Apple does not negotiate with its suppliers and (b) GTAT had to agree to all of Apple's material terms and the draft agreements prepared by Apple's attorneys, or the deal was off. Remarkably, Apple's chief legal negotiator on certain key aspects of the transaction was Apple's Senior (Bankruptcy) Restructuring Counsel. It goes without saying that this speaks volumes about Apple's perspective on the transaction it was about to enter into less than one year ago.

17. The following terms are illustrative of Apple's approach to the transaction:

- Apple required GTAT to commit to supply millions of units of sapphire material, but Apple has ***no obligation to buy*** any of that sapphire material.
- Apple required GTAT to form a wholly-owned subsidiary, Debtor GT Advanced Equipment Holding LLC ("GT Equipment"), in October 2013 to implement a convoluted and artificial structure that serves no economic purpose—other than protecting Apple—such that GTAT Corp. would be obligated to buy and assemble furnaces for Apple, but the cash and furnaces would then be "round-tripped" through GT Equipment, a so-called "bankruptcy remote entity" using an illusory sale and leaseback between GTAT Corp. and GT Equipment.
- Apple took a security interest in the entity referred to in the documents as the "bankruptcy remote entity," which Apple designed to hold the furnaces.
- GTAT was prohibited, for years to come, from conducting any sapphire business with any conceivable Apple competitor or any direct and indirect supplier to an Apple competitor.

18. The various agreements Apple presented to GTAT as a condition for a business collaboration with Apple are best described as "adhesion contracts." A "best of" collection of the contractual terms is provided below to explain what Apple, foisted on GTAT:

- If GTAT discloses any aspect of the agreements with Apple, it is liable for breach of confidentiality to Apple for ***$50 million per occurrence*** as liquidated damages; Apple, on the other hand, is not liable for any liquidated damages if it violates confidentiality.

- GTAT must accept and fulfill any purchase order placed by Apple on the date selected by Apple. If there is any delay, GTAT must either use expedited shipping (***at its own cost***) or purchase substitute goods (***at its own cost***). If GTAT's delivery is late, GTAT must pay **$320,000 per boule of sapphire** (and $77 per millimeter of sapphire material) as liquidated damages to Apple. To put this figure in perspective, a boule has a cost of less than $20,000. Apple, however, has the right, ***without compensating GTAT***, to cancel a purchase order in whole or in part at any time and reschedule a delivery date at any time.

- GTAT must pay **$640,000 per boule** that it sells to a third party in violation of the exclusivity restrictions in the contract. Apple has no obligation to buy boules exclusively from GTAT.

- GTAT must pay **$650,000 per month** for any sapphire furnace that is used in violation of GTAT's exclusivity obligations to Apple. To put this figure in perspective, furnaces provided as part of the transactions with Apple were provided at a one-time total cost of approximately $200,000 per furnace. Apple has no exclusivity obligations to GTAT.

- GTAT is prohibited from modifying any equipment, specifications, manufacturing process or materials without Apple's prior consent. Apple, on the other hand, can modify any of these terms at any time and GTAT must immediately implement Apple's modifications.

- If Apple exercises a Termination Event, and becomes a "lessee" of the furnaces and related equipment in the Mesa Facility, the rental amount Apple would pay to GT Equipment is **$50 per month**, as compared with the $9.9 million monthly rent payment that GTAT Corp. is "deemed" to pay to GT Equipment under its "lease" with GT Equipment.

- Apple enjoys an "exclusive right of negotiation," which is basically a provision that forces GTAT to negotiate exclusively with Apple for thirty days if it seeks to sell substantially all assets ***or*** its sapphire business ***or*** it receives an expression of interest from a third party. If GTAT violates this provision it must pay Apple **$1 billion**. Of course, Apple has no such corresponding obligation to GTAT.

- Apple cannot be liable to GTAT for any design defects or consequential damages from product flaws occurring at the Mesa Facility, which Apple owns, unless GTAT proves that the causes of those defects or flaws were ***solely*** Apple's fault.

- Apple drafted and structured 14 separate agreements purporting to reflect separate transactions among GTAT Corp., and its subsidiary, GT Equipment. But all of these agreements have cross-termination provisions that clearly show how Apple exercised control over the operations and assets related to this transaction.

- GTAT sends the sapphire material it produces to two of Apple's "captive" vendors in Asia. Those vendors further process the sapphire material into an end product. If there is a question about whether the sapphire product GTAT ships to Asia is defective, a "committee" of three parties, comprised of GTAT, Apple and one of the two "captive" vendor in Asia, answer that question, with each party getting one vote on whether GTAT was at fault or not. It is not difficult to see what the outcome of this vote would be.

- If Apple terminates the SOW (as defined herein) for cause, then GT Equipment must immediately repay the intercompany loan from GTAT Corp. By contrast, if GTAT Corp. terminates the SOW for cause, there is no acceleration of the loan obligations.

19. When GTAT's management expressed obvious concerns to Apple regarding the deal terms during the contract negotiations, Apple responded that similar terms are required for other Apple suppliers and that GTAT should: "Put on your big boy pants and accept the agreement." At the same time, however, Apple expressed its commitment to sapphire technology and its intention to work collaboratively with GTAT to bring the technology to fruition in a manner that would have allowed GTAT to produce sapphire materials consistent with the terms and conditions of the agreements in an economically viable manner.

20. At the closing of the Apple transaction, GTAT also took on substantial new debt. Specifically, on or about October 30, 2013—the day before the agreements with Apple were signed—GTAT terminated its revolving credit agreement with Bank of America and paid off all outstanding debt owed to Bank of America at that time. This was necessary to permit Apple to take a lien on all of the assets of both GTAT Corp. and GT Equipment—yet another deal term that Apple demanded.

21. As permitted by the Apple agreements, GTAT borrowed an additional $214 million by issuing additional convertible notes in 2013 and raised $71 million through a concurrent common stock sale.

Once Apple Agreements are Signed, Apple Dictates Sapphire Growth and Fabrication Processes

22. From day one, Apple was intimately involved in (and, in many instances, controlled) key aspects of the sapphire growth and fabrication processes.

23. A specialized facility is required to house over 2,000 sapphire furnaces and the related fabrication equipment. In addition, due to the nature of sapphire growth, a stable and uninterrupted power infrastructure and supply of process cooling and emergency water is required because interruptions in power or cooling water can render the sapphire-growth materia unusable, causing millions of dollars in losses.

24. Apple selected the Mesa Facility and negotiated all power and construction contracts to design and build out the facility with third parties. In fact, GTAT was prohibited from having direct communications with the Apple subcontractors that were building out the Mesa Facility. Ultimately, the first phase of the Mesa Facility was not operational until December 2013—which was only 6 months before GTAT was expected to be operating at full capacity in order to meet its "Minimum Supply Commitments" (as defined in the SOW).

25. Additional unplanned delays continued to surface, because the Mesa Facility required a significant amount of reconstruction, including reconstruction of floors roughly the size of multiple football fields. The build-out of the Mesa Facility, delays in available power, and power interruptions, further delayed the ramp-up of sapphire growth and fabrication by approximately three months. This was critical lost time during which GTAT could not begin

manufacturing sapphire for sale to Apple and recoup its massive investment in furnaces for Apple.

26. Further complicating GTAT's build-out of sapphire-growth furnace and fabrication areas, there were over 1,200 construction workers engaged in the build-out of the Mesa Facility—an impossible situation given the need to be producing at full capacity by Summer 2014. This ongoing construction project also meant that GTAT was operating in a highly contaminated environment that adversely affected the quality of sapphire material.

27. The quality and reliability of the power infrastructure, as noted earlier, is critical to the sapphire growth process. Prior to entering into the Apple Agreements, GTAT advised Apple that the implementation of uninterruptable power systems and generators was essential, particularly in an operation with 2,036 furnaces. GTAT advised Apple that even a brief interruption of power could result in a loss of potentially more than $30 million to GTAT. After much discussion, Apple determined that implementing power back-up for the furnaces was too expensive and, therefore, "non-essential." After the Mesa Facility was finally operational, GTAT's concerns about the reliability of the power supply were realized. On at least three occasions, power interruptions occurred, leading to significant delays and losses of whole production runs of sapphire boules. GTAT's losses to date resulting from power outages at the Mesa Facility exceed $10 million. These power interruptions also adversely affected GTAT's ability to develop and optimize the process for growing sapphire material to Apple's changing specifications because GTAT lost important data every time a boule was damaged by a furnace run affected by interruptions of power or water.

28. In addition, Apple sent a significant number of employees to the Mesa Facility and the Salem Facility, including supply chain, manufacturing, and quality engineers—most of

them having no prior experience in sapphire growth or fabrication. These Apple employees were involved on a full-time basis in GTAT's sapphire growth and fabrication processes, taking up as much as 30% of GTAT's R&D and manufacturing team's time. These employees also assumed a level of authority in the Mesa Facility and Salem Facility that was disruptive and prevented GTAT from managing its operations as it saw fit. On multiple occasions, GTAT had to remind the onsite Apple team that they were not to give directions to GTAT employees.

29. Many of the processes associated with cutting, polishing, and shaping sapphire (this is the "fabrication process", in contrast to the "growth process" that takes place in the furnaces) were new, given the unprecedented volume of sapphire being grown at the Mesa Facility. It was Apple, however, that dictated to GTAT what tools to use and what fabrication processes to implement at the Mesa Facility. Apple also worked directly with suppliers of cutting and polishing equipment to specify and in some cases develop such tools, but, prior to contract signing, explicitly prohibited GTAT from having direct contact with these suppliers.

30. The fabrication methods specified by Apple prevented GTAT from achieving its planned fabrication cost and production targets because many of the tools did not meet their performance and reliability specifications by a wide margin. For example, the diamond wire tool intended to cut sapphire boules was specified to perform this task in 3.6 hours; however, the tool selected by Apple had significant operating issues resulting in a process that took more than 20 hours. Ultimately, that tool was unsuitable for the task and had to be replaced by a different tool. In fact, a majority of the fabrication tools dictated by Apple had to be replaced with alternative tools, resulting in additional capital investment and operating costs to GTAT and months of lost time in production. The fabrication cost is approximately 30% higher than planned, requiring nearly 350 additional employees and significantly higher consumption of diamond wire and

other wear items than originally planned. A few weeks before the Petition Date, Apple made clear that it refused to accept any financial responsibility for these issues, making it clear that it expected GTAT to absorb these additional costs in spite of the fact that Apple dictated the selection of all of the tools that created the problems.

31. Next, Apple withheld the final prepayment of **$139 million**. In August 2014, Apple acknowledged that it would make the final prepayment if GTAT were to grow sapphire boules in accordance with certain revised specifications. Shortly after that acknowledgement, however, Apple reversed course, requiring that GTAT satisfy the original specifications—which Apple knew GTAT could not meet under the circumstances.

32. When GTAT initially entered into negotiations to sell sapphire furnaces to Apple, it had no sense that this relationship would become a "heads I win, tails you lose" proposition for Apple. But, having borrowed hundreds of millions of dollars to pay for the components of more than 2,036 sapphire furnaces, GTAT was essentially powerless to stop Apple's control, regardless of whether Apple had a contractual right to exercise control or not.

33. Unfortunately, these chapter 11 cases are not just a dispute between two parties—otherwise GTAT might have been able to redress this matter through litigation with Apple. At bottom, all of GTAT's stakeholders are the victims of Apple's inequitable conduct. GTAT has numerous creditors at various levels of its corporate structure. Notably, GT (GTAT's parent company) is obligor under more than $430 million in convertible notes, a significant portion of which Apple required to be used to finance GTAT's consummation of the Apple transactions. Moreover, trade creditors hold approximately $145 million in claims against certain GTAT entities. Finally, GT's public shareholders have borne the brunt of Apple's "bait and switch

strategy" and have seen their investment in what appeared to be a promising technology venture thwarted by Apple.

34. In many ways, Apple, through its unrelenting control of material aspects of sapphire growth and fabrication has converted GTAT from a supplier/seller of furnaces into an experimental research and development venture for Apple funded substantially by GTAT's other stakeholders.

35. In light of the interests of these creditors and other stakeholders, and given the severity of the losses incurred as a result of the transactions with Apple, GTAT had little choice but to commence these chapter 11 cases.

36. Despite Apple's very recent protestations to the contrary, Apple was aware, at all relevant times, of the financial condition of GTAT and of the fact that GTAT was losing substantial amounts on each sale of sapphire product to Apple. Moreover, as recently as a few weeks ago, GTAT senior management made a detailed presentation to Apple senior management in charge of the sapphire growth project and advised them very clearly that GTAT was losing substantial amounts and that it was projected to run out of cash in a few weeks.

Sapphire Segment

37. In 2010, the GTAT Group acquired Crystal Systems Inc., which enabled the GTAT Group to enter the sapphire material and equipment business, with a focus on providing sapphire furnaces for the global LED and certain other industrial markets. GTAT's sapphire business was traditionally based on designing and selling advanced sapphire crystallization furnaces ("ASF"®), which are used to produce sapphire boules. These sapphire boules are used, following certain cutting and polishing processes, to make sapphire wafers, a substrate for manufacturing light emitting diodes, as well as sapphire material for a wide range of other

industrial and consumer applications including, medical devices, dental, oil and gas, watch crystals, and specialty optical applications such as low absorption optical sapphire for advanced optics and titanium-doped sapphire material for high power lasers.

38. Sapphire is one of the hardest substances on Earth. It is scratch-resistant, and can be produced in highly transparent form. Given its strength and make-up, sapphire is an ideal material to replace the glass screens currently used in today's most popular consumer electronic products, such as smartphones, which are prone to cracking and scratching. Virtually every consumer has, at some time, experienced the frustration of a scratched or cracked smartphone screen. The market has been intensely interested in sapphire as a remedy for these common problems. Sapphire is also believed to use less power than common glass screens, making it an even more ideal replacement for glass screens used in portable consumer electronic products like smartphones.[3]

Business Relationship with Apple[4]

39. On October 31, 2013, GTAT entered into the Apple Agreements with Apple. The Apple Agreements shifted the GTAT Group's sapphire business model from being primarily an equipment manufacturer to also being a sapphire materials manufacturer.

---

[3] For an illustration of how sapphire is manufactured, see https://www.youtube.com/watch?v=vsCER0uwiWI

[4] As a result of the transactions entered into between GTAT and Apple, GTAT Corp. is subject to numerous confidentiality obligations under agreements with Apple (collectively, the "Confidentiality Obligations"). The Confidentiality Obligations broadly preclude GTAT Corp. from disclosing information concerning the nature of GTAT Corp.'s business relationship with Apple and other nonpublic information related thereto. These agreements further provide that each breach of the Confidentiality Obligations will require GTAT Corp. to pay liquidated damages to Apple in an amount of **$50 million per occurrence.** However, these agreements permit GTAT Corp. to disclose confidential information "to the extent required by law," provided GTAT Corp. makes reasonable efforts to give Apple notice of such requirement prior to any such disclosure and take reasonable steps to obtain protective treatment of the confidential information. Concurrently, herewith GTAT has filed a motion seeking either (a) entry of an order authorizing GTAT to file an unredacted version of the Supplemental First Day Declaration under seal or (b) entry of an order directing GTAT to file an unredacted Supplemental First Day Declaration on the Court's docket.

40. Under the Apple Agreements, Apple agreed to advance approximately $578 million, essentially as a loan to GTAT Corporation ("GTAT Corp.") to enable GTAT Corp. to build 2,036 ASF furnaces in the Mesa Facility. Apple structured the deal to ensure that GTAT could only supply sapphire to Apple—and none of Apple's competitors. Apple, acting like a lender rather than a customer, also required GTAT Corp. (a) to form a special purpose subsidiary which was to hold title to the ASF furnaces and related equipment and (b) to pledge its interest in that subsidiary as collateral to secure repayment of the $578 million advance. The most relevant Apple Agreements are summarized below.

41. MDSA and Statement of Work. On October 31, 2013, GTAT Corp. and Apple entered into a Master Development and Supply Agreement and related Statement of Work ("SOW"), pursuant to which the GTAT Group agreed to supply sapphire material to Apple. While the MDSA specifies the GTAT Group's minimum and maximum supply commitments, Apple has no purchase requirements under the terms of the MDSA, despite the fact that GTAT had to acquire and install 2,036 furnaces worth millions of dollars at the Mesa Facility.

42. Prepayment Agreement. Also on October 31, 2013, GTAT Corp. entered into a Prepayment Agreement with Apple pursuant to which the GTAT Corp. was eligible to receive $578 million in four separate installments, as a loan to pay for the purchase of sapphire furnaces and other equipment required under the MDSA and related SOW. GTAT Corp. is required to repay this amount ratably over a five year period commencing in 2015 and ending in January 2020, either as a credit against amounts due from Apple purchases of sapphire material under the MDSA or as a direct cash payment. No interest accrues on the loan from Apple under the Prepayment Agreement. The installment payments received by GTAT Corp. were to be used exclusively by GTAT Corp. to fund the purchase of components necessary to manufacture 2,036

ASF furnaces and related processing and manufacturing equipment at the Mesa Facility, which is owned by an affiliate of Apple and leased to GTAT Corp.

43. The first three installments under the Prepayment Agreement of $225 million, $111 million, and $103 million were received on November 15, 2013, January 23, 2014, and April 4, 2014, respectively. As of the Petition Date, the fourth and final installment payment, in the amount of $139 million, has not been received by GTAT Corp., even though GTAT had completed installation of 2,036 furnaces at the Mesa Facility.

44. Formation and Pledge of Special Purpose Entity. As part of the Prepayment Agreement, GTAT Corp. was also required to form a Delaware limited liability company as a wholly-owned subsidiary, which Apple attempted to design to be "bankruptcy remote." Accordingly, GTAT Corp. formed GT Equipment in October 2013. As collateral for its obligations under the Prepayment Agreement, the MDSA and the SOW, GTAT Corp. entered into a Membership Interest Pledge Agreement, dated October 31, 2013 (the "Pledge Agreement"), under which it pledged its membership interest in GT Equipment to Apple. GT Equipment is one of the Debtors in these chapter 11 cases.

45. Intercompany Loan Agreement. To the extent GTAT Corp. received funds under the Prepayment Agreement, GTAT Corp. was obligated to make an intercompany loan to GT Equipment in the amount of the payment from Apple pursuant to that certain Loan Agreement, dated October 31, 2013 between GTAT Corp. and GT Equipment (the "Intercompany Loan Agreement"). The Intercompany Loan, like the loans under the Prepayment Agreement, has a 0% interest rate. GT Equipment is required to repay the loan over five years in 58 equal monthly installments of $9,965,517.24. In addition, GT Equipment's obligations under the Intercompany Loan Agreement are not contractually subordinated to GT Equipment's obligations to Apple.

46. GT Equipment was supposed to use the funds loaned by GTAT Corp. to purchase component parts to construct the 2,036 furnaces at the Mesa Facility, related equipment, supplies or other operational expenditures related to Apple (the "Mesa Equipment"). In practice, however, GT Equipment did nothing. GTAT Corp. ordered all furnace parts and paid all third party and related suppliers of the furnace components, and GT Corp. installed all 2,036 furnaces at the Mesa Facility. Moreover, the transfers between GTAT Corp. and GT Equipment were completely circuitous because every dollar transferred by GTAT Corp. to GT Equipment was round-tripped back to GTAT Corp. Therefore, when the dust settled, Apple loaned funds to GTAT Corp., GTAT Corp. loaned funds to GT Equipment, and GT Equipment returned the money right back to GTAT Corp.

47. Apple and GTAT Corp. also entered into a Conditional Assignment, dated October 31, 2013 (the "Conditional Assignment"), under which GTAT Corp. assigned to Apple all its right, title and interest (but not its obligations) in the Intercompany Loan Agreement. However, and importantly, this assignment is not effective until the occurrence of (i) a Trigger Event (as defined below) under the Prepayment Agreement, (ii) GTAT Corp.'s receipt of a notice of default under the SOW or the MDSA, or (iii) an event of default under the Intercompany Loan Agreement. None of these Trigger Events occurred prior to the Petition Date.

48. Equipment Lease Agreements. As purported owner of the Mesa Equipment, GT Equipment entered into a Lease Agreement with GTAT Corp., dated October 31, 2013 (the "GT Equipment Lease"), under which GT Equipment leased the Mesa Equipment to GTAT Corp.[5]

[5] The GTAT Equipment Lease would terminate upon, among other things, a termination of the SOW by Apple for cause or the occurrence of so-called "Trigger Events" under the Prepayment Agreement which allow Apple to, among other things, accelerate repayment of amounts advanced to GTAT Corp. under the Prepayment Agreement. No Trigger Event occurred prior to the Petition Date.

The rent under GT Equipment Lease is equal to the amount of the Intercompany Loan Repayment that GT Equipment owed to GTAT Corp. under the Intercompany Loan Agreement. Consequently, GTAT Corp. offsets its rental obligations against GT Equipment's obligations under the Intercompany Loan Agreement and no cash is exchanged. The practical effect of this aspect of the agreement is that GT Equipment "repays" the loan to GTAT Corp., at no cost, by offsetting rent payments under the GT Equipment Lease.

49. GT Equipment and Apple also entered into a "contingent" lease agreement, dated October 31, 2013 (the "Contingent Lease Agreement") for the Mesa Equipment. The Contingent Lease Agreement purports to be effective from the date GT Equipment purchases the Mesa Equipment until the earlier of (a) termination of the Contingent Lease Agreement, (b) the Mesa Equipment is no longer property of GT Equipment, (c) expiration or termination of either the MDSA or the SOW. However, Apple is not entitled to take possession of the Mesa Equipment unless and until the GT Equipment Lease is terminated. If Apple took possession of the Mesa Equipment, the rental amount would be **$50 per month**, as compared with the **$9.9 million** deemed monthly rent payment that GTAT Corp. pays to GT Equipment. The GT Equipment Lease had not terminated as of the Petition Date.

50. GT Equipment Secured Guaranty. On October 31, 2013, GT Equipment issued a secured guaranty in favor of Apple guaranteeing all of GTAT Corp.'s obligations under the Prepayment Agreement, the MDSA, or the SOW (the "Secured Guaranty"). GT Equipment granted Apple a first-priority security interest in all of its assets. GT Equipment's obligations under the Secured Guaranty become due when either (i) Apple terminates the SOW for cause or (ii) a Trigger Event occurs under the Prepayment Agreement.

51. Security Agreement. Apple and GTAT Corp. also entered into a Security Agreement, dated October 31, 2013 (the "Security Agreement") pursuant to which GTAT Corp. granted Apple a security interest and lien on certain of GTAT Corp.'s assets. However, Apple's lien and security interest were extinguished pursuant to the Security Agreement when GT issued the convertible notes described below and contributed proceeds of the note issuance to GT Equipment. Therefore, as of the Petition Date, the only asset of GTAT Corp. which constitutes collateral of Apple is the LLC membership interest in GT Equipment. This means that Apple does not have a so-called "back-up" security interest against the assets of GTAT Corp.,[6] which lenders to special purpose entities generally insist on in the event the special-purpose-entity structure is disregarded, or if the assets supposedly owned by the special purpose entity are found to be the property of its parent.[7]

52. Mesa Facility Lease. GTAT Corp., not GT Equipment, entered into a lease for the Mesa Facility on October 31, 2013. The landlord at the Mesa Facility is Platypus Development LLC, an affiliate of Apple ("Platypus"). GTAT Corp. pays $100 per year as rent to Platypus for use of the Mesa Facility. Consequently, when furnaces were delivered to, and assembled at, the Mesa Facility, they were delivered to GTAT Corp., not GT Equipment.

SUPPORT FOR RELIEF REQUESTED IN ADDITIONAL FIRST DAY PLEADINGS

53. Concurrently with the filing of Supplemental Declaration, or as soon as practicable thereafter, GTAT has filed (or will file) a number of Additional First Day Pleadings

---

6 This could become relevant because, despite the numerous agreements which attempt to document the relationship between Apple and GTAT, Apple never insisted on, and it does not appear that there are any, purchase agreements or bills of sales executed between GT Corp. and GT Equipment to reflect the "purchase" by GT Equipment from GT Corp. of the furnaces. GT Corp., and not GT Equipment, ordered the furnace parts from the third party vendors and paid such third party vendors for all the parts for the furnaces GT Corp. installed in the Mesa Facility, and the furnaces were installed in a location where GT Corp., not GT Equipment, was the tenant. In the interest of full disclosure, GT, the ultimate parent of both GT Corp. and GT Equipment, reflected the furnaces located at the Mesa Facility as assets of GT Equipment in its public filings.

seeking relief that GTAT believes is necessary to enable it to operate with minimal disruption and loss of productivity. The facts set forth in the Additional First Day Pleadings are incorporated by reference in their entirety. GTAT requests that the relief requested in each of the Additional First Day Pleadings be granted as critical elements in ensuring a smooth transition into chapter 11.

54. I have reviewed each of the Additional First Day Pleadings, and the facts stated therein are true and correct to the best of my belief with appropriate reliance on corporate officers and advisors. The relief sought in each of the Additional First Day Pleadings is necessary to enable GTAT to continue operations with minimal disruption and constitutes a critical element in the successful implementation of GTAT's effort to maximize the recovery of its creditors. To this end, GTAT has filed the following Additional First Day Pleadings:

a. **Debtors' Emergency Motion for (A) Entry of Order, Pursuant to Bankruptcy Code Section 107(b) and Bankruptcy Rule 9018, Authorizing Filing Under Seal of Unredacted Versions of Supplemental First Day Declaration and Motion to Reject, or (B) Alternatively, Entry of Order, Pursuant to Bankruptcy Code Sections 105(a) and 107(a) Directing Debtors to File Unredacted Versions Thereof;**

b. **Debtors' Emergency Motion for Entry of Order, Pursuant to Bankruptcy Code Section 107(b) and Bankruptcy Rule 9018, Authorizing Filing of Motion to Seal Under Seal;**

c. **Debtors' Emergency Motion Pursuant to Bankruptcy Code Sections 105(a) and 365(a) for Entry of Order Authorizing Debtors to Reject Certain Executory Contracts and Unexpired Leases *Nunc Pro Tunc* to the Petition Date;**

d. **Debtors' Emergency Motion, Pursuant to Bankruptcy Code Sections 105(a) and 363(b), for Entry of Order (I) Authorizing Debtors to Wind Down Operations at Sapphire Manufacturing Facilities and (II) Approving Wind Down Employee Incentive Plan in Connection with Wind Down of Such Operations; and**

e. **Debtors' Emergency Motion for Expedited Hearing on Debtors' (I) Motion to Wind Down Operations, (II) Reject Certain Executory**

Contracts and Unexpired Leases in Connection with Such Wind Down, (III) Motion to Seal Foregoing Motions and Supplemental First Day Declaration, and (IV) Motion to Seal the Sealing Motion.

CONCLUSION

55. I believe approval of the relief requested in the Additional First Day Pleadings is in the best interests of all stakeholders.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing statements are true and correct.

Dated: October 8, 2014

On behalf of GTAT

By: Daniel W Squiller
Name: Daniel W. Squiller
Title: Chief Operating Officer

LIST OF REFERENCES

The Acquisition Handbook, Edition 4. Bardwell, England: Tactica Solutions, 2002. http://www.defence.org.cn/aspnet/vip-usa/uploadfiles/2004102932134509.pdf.

Adams, John. *Remaking American Security: Supply Chain Vulnerabilities & National Security Risks across the U.S. Defense Industrial Base*. Washington, DC: Alliance for American Manufacturing, 2013. http://s3-us-west-2.amazonaws.com/aamweb/uploads/research-pdf/RemakingAmericanSecurityMay2013_2.pdf.

American Bar Association Public Contract Law Section. "A White Paper Regarding Department of Defense Implementation of Section 818 of the National Defense Authorization Act for Fiscal Year 2012." White paper, American Bar Association, 2012.

Apple. "Apple Supplier Code of Conduct." January 1, 2017. https://images.apple.com/supplier-responsibility/pdf/Apple-Supplier-Code-of-Conduct-January.pdf.

———. "Supplier Responsibility: 2017 Progress Report." March 2017. https://www.apple.com/supplier-responsibility/.

Auger, Martin. *Defense Procurement Organizations: A Global Comparison*. Publication No.2014-82-E. Ottawa, Canada: Library of Parliament, 2014. https://lop.parl.ca/Content/LOP/ResearchPublications/2014-82-e.pdf.

Betti, Stafano, and Rosella Mangion. "Prosecuting Counterfeiting and Organised Crime: The Need for a Creative Legal Approach." In *Anti-counterfeiting 2014: A Global Guide*. World Trademark Review, 2014.

Bullock, J., A. Hudson, R. Matthews, C. Elliot, and D. Greenwood. *Counterfeit Avoidance Maturity Model* (Version1). Bristol, UK: Ministry of Defense, 2015. https://www.erai.com/CustomUploads/ca/wp/Counterfeit_Avoidance_Maturity_Model.pdf.

Bostock, John. *Pliny the Elder, The Natural History*. London: Taylor and Francis, 1855. http://www.perseus.tufts.edu/hopper/text?doc=Perseus:abo:phi,0978,001:33.

Chaudhry, Peggy, and Alan Zimmerman. *Protecting Your Intellectual Property Rights*. New York: Springer-Verlag, 2013.

Frontier Economics. "The Economic Impacts of Counterfeiting and Piracy." Report, International Chamber of Commerce, 2016. https://cdn.iccwbo.org/content/uploads/sites/3/2017/02/ICC-BASCAP-Frontier-report-2016.pdf.

Gansler, Jacques S., William Lucyshyn, and Lisa H. Harrington. "An Analysis of Through Life Support Capability Management at the U.K.'s Ministry of Defense." Report, University of Maryland Center for Public Policy and Private Enterprise, 2012. https://www.dau.mil/cop/pbl/DAU%20Sponsored%20Documents/UMD%20FINAL%20Report%20LMCO%20An%20Analysis%20of%20Through%20Life%20Support%20Capability%20Management%20at%20the%20UK%20s%20Ministry%20of%20Defense%20June%202012.pdf.

Gansler, Jacques S., William Lucyshyn, and John Rigilano. "Addressing Counterfeit Parts in the DOD Supply Chain." Report, University of Maryland Center for Public Policy and Private Enterprise, 2014. https://calhoun.nps.edu/bitstream/handle/10945/45074/UMD-LM-14-012.pdf?sequence=1.

Gates, Susan M., Elizabeth Roth, Sinduja Srinivasan, and Lindsay Dagherty. *Analyses of the Department of Defense Acquisition Workforce: Update to Methods and Results through FY 2011*. Santa Monica, CA: RAND, 2013. http://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR110/RAND_RR110.pdf.

Government Accountability Office (GAO). *Counterfeit Parts: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk*. GAO-16-236. Washington, DC: GAO, 2016. https://www.gao.gov/assets/680/675227.pdf.

———. *DOD Supply Chain: Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms*. GAO-12-375. Washington, DC: GAO, 2012. http://gao.gov/products/GAO-12-375.

———. *Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*, GAO-10-423. Washington, DC: GAO, 2010.

Gray, Bernard. "Review of Acquisition for the Secretary of State for Defense." Independent report, BiP Solutions, 2009. https://www.bipsolutions.com/docstore/ReviewAcquisitionGrayreport.pdf.

Hambleton, Ken, David Kirkpatrick, Ian Holder, David Kimberely, Mike, Bragg, Steve Mcinally, Alex Weiss, and Tim Williams. *Conquering Complexity Lessons for Defence Systems Acquisition*. London: The Defence Engineering Group, 2005.

Hillman, Richard J. *DOD Supply Chain: Preliminary Observations Indicate that Counterfeit Electronic Parts Can be Found on Internet Purchasing Platforms*. GAO-12-213T. Washington, DC: GAO, 2011. http://www.gao.gov/assets/590/586136.pdf.

Institute of Electrical and Electronics Engineers (IEEE). "IEEE Reliability Society Technical Operations Annual Technology Report for 2008." *IEEE Transactions on Reliability* 58, no. 2 (June 2009): 210–261. http://ieeexplore.ieee.org/document/5062554/.

Issacson, Walter. *Steve Jobs*, e-book. New York: Simon Schuster, 2011.

Mark, Ken. *Apple Inc.: Managing A Global Supply Chain*. Ontario, Canada: Ivey Publishing.

Martin, Theodore H. "The Globalization of America's Defense Industries: Managing the Threat of Foreign Dependence." *International Security* 15, n.o. 1 (Summer 1990): 57–99. https://www.jstor.org/stable/pdf/2538982.pdf?refreqid= excelsior%3A1188b7db5e859981aed8817ca6ba5440.

Mentzer, John T., William Dewitt, James S. Keebler, Soonhong Min, Nancy W. Nix, Carlo D. Smith, and Zach G. Zacharia. "Defining Supply Chain Management." *Journal of Business Logistics* 22, no. 2 (September 2001): 1–25.

National Audit Office. *Transforming Logistics Support for Fast Jets*. London: The Stationery Office, 2017. https://www.nao.org.uk/wp-content/uploads/2007/07 /0607825.pdf.

Organization of Economic Cooperation and Development. *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact*. Paris: OECD Publishing, 2016.

Schwartz, Moshe. *Defense Acquisitions: How DOD Acquires Weapons Systems and Recent Efforts to Reform the Process*. CRS Report No. RL34026. Washington, DC: Congressional Research Service, 2014. https://fas.org/sgp/crs/natsec/ RL34026.pdf.

Yin, Robert K. *Case Study Research: Design and Methods*. Los Angeles: SAGE, 2014.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California