

December 2012

Counterfeit Electronic Parts and the Lanham Act

Garrett Tozier

Follow this and additional works at: <https://scholarship.law.ufl.edu/jtlp>

Recommended Citation

Tozier, Garrett (2012) "Counterfeit Electronic Parts and the Lanham Act," *Journal of Technology Law & Policy*. Vol. 17: Iss. 2, Article 4.

Available at: <https://scholarship.law.ufl.edu/jtlp/vol17/iss2/4>

This Note is brought to you for free and open access by UF Law Scholarship Repository. It has been accepted for inclusion in *Journal of Technology Law & Policy* by an authorized editor of UF Law Scholarship Repository. For more information, please contact kaleita@law.ufl.edu.

NOTE

COUNTERFEIT ELECTRONIC PARTS AND THE LANHAM ACT

*Garrett Tozier**

I.	INTRODUCTION	329
II.	COUNTERFEIT PARTS IN THE DEFENSE SUPPLY CHAIN	332
	A. <i>The Defense Supply Chain</i>	332
	B. <i>Efforts to Eliminate Counterfeit Electronic Parts</i>	334
III.	LANHAM ACT APPLICATION TO COUNTERFEIT MARKS.....	340
IV.	ALTERNATIVE MEANS FOR ACHIEVING NDAA 2012's INTENDED PURPOSE	344
	A. <i>Clarifying the "Counterfeit" Definition</i>	345
	B. <i>Alternative Sources of Liability</i>	348
V.	CONCLUSION.....	351

I. INTRODUCTION

While certain provisions of the National Defense Authorization Act for Fiscal Year 2012¹ (NDAA 2012) have caused some controversy,² the more than 500 page bill has numerous national defense provisions which both Democrat and Republican leaders considered necessary.³ One particular section of the NDAA 2012 that received strong

* J.D. May 2013, University of Florida Levin College of Law; B.S., University of Florida, 2010. I would like to thank my family for their tremendous support.

1. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, 125 Stat. 1298 (2012) [hereinafter NDAA 2012].

2. See Statement on Signing the National Defense Authorization Act for Fiscal Year 2012, 2011 DAILY COMP. PRES. DOC. 978 (Dec. 31, 2012) (expressing the Obama Administration's reservations with certain provisions of the NDAA 2012 related to the detention, interrogation, and prosecution of suspected terrorists).

3. See *id.* (recognizing the NDAA 2012's importance in modernizing the national defense and boosting the effectiveness of military operations worldwide); 157 CONG. REC. S7643-48 (daily ed. Nov. 17, 2011) (statements of Sen. Carl Levin and Sen. John McCain) (introducing amendment 1092 to the NDAA 2012 and noting the strong bipartisan support of section 818).

bipartisan support during the drafting and passage of the bill addressed the growing concern with counterfeit electronic parts⁴ entering the defense supply chain.⁵ In multiple instances prior to the passage of NDAA 2012, the Department of Defense (DoD) discovered thousands of unique parts and materials that contained counterfeit electronic parts provided by hundreds of suppliers.⁶ Therefore, Congress added section 818 to the NDAA 2012 to address problems related to the detection and avoidance of counterfeit electronic parts throughout the defense supply chain.⁷ Section 818 authorized the Secretary of Defense to create acquisition policies and systems for the detection and avoidance of counterfeit electronic parts and established criminal penalties for the use of counterfeit electronic parts.⁸

Congress codified the criminal offenses for trafficking in counterfeit military goods or services under section 2320 of title 18, U.S. Code.⁹ Similar criminal offenses for trafficking in counterfeit goods under section 2320 are based on trademark principles established by the Lanham Act,¹⁰ and the NDAA 2012's revisions to section 2320 draw from these principles as well.¹¹ And while at the time of this writing the Secretary of Defense has yet to amend DoD acquisition policies and systems for the detection and avoidance of counterfeit electronic parts,¹²

4. Section 818 defines an "electronic part" as "an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, resistor, or diode,) or a circuit assembly." NDAA 2012, § 818(f)(2).

5. *Id.* § 818, 25 Stat. at 1493–1500. *See also* 157 CONG. REC. S7647 (daily ed. Nov. 17, 2011) (statement of Sen. John McCain) (regarding amendment 1092 to the NDAA 2012).

6. *See National Defense Authorization Act for Fiscal Year 2012 and the Future Years Defense Program: Hearing on S. 1253 Before the S. Comm. on Armed Servs.*, 112th Cong. 228–29 (2011) (statement of Patrick J. O'Reilly, Lieutenant General, USA). The large number of counterfeit parts throughout the defense supply chain required numerous recalls. *Id.*

7. NDAA 2012, § 818, 125 Stat. at 1493–1500.

8. *Id.* § 818(a)-(e), (h), 125 Stat. at 1493–96, 1497–1500.

9. *Id.* § 818(h), 125 Stat. at 1497–1500.

10. 15 U.S.C. §§ 1051–1127 (2006).

11. *See* 18 U.S.C. § 2320(d), (f)(3) (2012) (defining the Lanham Act and those charged with violations of section 2320 to assert any defenses that would be available under the Lanham Act).

12. While the official definition has not been promulgated at the time of this writing, the Under Secretary of Defense for Acquisition, Technology and Logistics issued memoranda detailing internal expectations regarding the detection and avoidance of counterfeit items, including definitions of "counterfeit material" and "suspect parts." *See* Memorandum from Acting Undersecretary of Defense for Acquisition, Tech. and Logistics Frank Kendall to Sec'y. of the Military Dep'ts. and Dirs. of the Def. Agencies, Overarching DoD Counterfeit Prevention Guidance (Mar. 16, 2012), *available at* <http://www.dmsms2012.com/images/Counterfeit-Prevention-Guidance.pdf> (defining "counterfeit material"); Memorandum from Acting Undersecretary of Defense for Acquisition, Tech. and Logistics Frank Kendall, DoD Supply Chain Material Management Policy (Dec. 14, 2011), *available at* <http://www.dtic.mil/whs/directives/corres/pdf/414001p.pdf> (defining "counterfeit material" and "suspect part"). Although

the Lanham Act will certainly be considered in drafting and promulgating those regulations.¹³

But despite Congress's intent of promoting safety throughout the defense supply chain by passing section 818 through the promulgation of counterfeit prevention regulations and the increased criminal penalties of section 2320,¹⁴ the DoD faces various problems in effectively implementing section 818. Those throughout the defense contracting industry have criticized the rule-making process thus far, noting the lack of formal or public process to solicit comments related to the development of the rules required by section 818.¹⁵ Industry organizations have already endorsed proposed amendments to section 818 contained in the NDAA 2013 reducing the costs imposed to contractors who comply with regulations.¹⁶ In addition to the opposition, certain trademark principles codified in the Lanham Act may create some unintended outcomes that may hamper the fight against counterfeit electronic parts in the defense supply chain.

This Note addresses the potential conflicts between Congress's intent in eliminating counterfeit electronic parts from the defense supply chain and the use of criminal penalties that rely upon the Lanham Act's trademark principles to achieve these ends. Following the introduction, Part II discusses the defense supply chain and the pervasiveness of counterfeit electronic parts throughout it. Part III analyzes section 2320 in the context of related Lanham Act principles, along with relevant case law applying to government contractors trafficking in counterfeit goods. Part IV provides suggestions for implementing the section 818 regulations and introduces alternative theories of liability that could

not explicitly stated, these memoranda may be an attempt to fulfill the DoD's requirement under NDAA 2012 section 818(b)(1) to "establish Department-wide definitions of the terms 'counterfeit electronic part' and 'suspect counterfeit electronic part.'" NDAA 2012 § 818(b)(1), 125 Stat. at 1493-94.

13. *Id.* § 818(g), 125 Stat. at 1496-97.

14. See 157 CONG. REC. S7643-48 (daily ed. Nov. 17, 2011) (statements of Sen. Carl Levin and Sen. John McCain) (stating that amendment 1092 to the NDAA 2012 will address the problem that counterfeit electronic parts entering the defense supply chain present to the safety and security of armed service members).

15. Robert S. Metzger, *Counterfeit Parts: What to Do Before the Regulations (and Regulators) Come? Practical Steps Industry Can Take Now*, 98 FED. CONTRACTS REPORTER 246, 1 (2012). The DoD has already delayed the promulgation of these regulations past the due date set by Congress, so it may be unclear whether the DoD will forego a comment period on these regulations. See NDAA 2012 § 818(b), 125 Stat. at 1493-94 (requiring promulgation of contractor regulations within 270 days of the passage of section 818, September 26, 2012); DEP'T OF DEF., OPEN DFARS CASES 3 (Oct. 26, 2012), available at <http://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf> (stating that in case number 2012-D055, at the time of this writing, that October 31, 2012 was the extended report date for a draft proposed rule of section 818 requirements).

16. Metzger, *supra* note 15, at 6-7.

better serve Congress's intent of eliminating counterfeit electronic parts in the defense supply chain.

II. COUNTERFEIT PARTS IN THE DEFENSE SUPPLY CHAIN

Every year the U.S. Government invests substantial energy and resources into each branch of the armed services and an effective supply chain is an integral part in the military's ability to operate efficiently and execute its global operations.¹⁷ As with most consumer goods, the U.S. Government has a vital interest in protecting the military from using unsafe military weapons.¹⁸ Part A of this Part will describe the defense supply chain and the growth of counterfeit electronic parts found within it. Part B of this Part details previous efforts of detecting counterfeit goods in the United States and compares past efforts with section 818's goal of eliminating counterfeit electronic parts from the defense supply chain.

A. *The Defense Supply Chain*

In order to understand the section 818's goals of eliminating counterfeit electronic parts from the defense supply chain it is important to understand how the defense supply chain operates. Various government agencies provide support for the U.S. Military, and these agencies can focus their efforts on providing a specific type of military supplies or supplying a specific branch of the military.¹⁹ But regardless each agency's focus, the procurement, storage and distribution of electronic parts are integral responsibilities for operation of a safe and effective defense supply chain.

The Defense Logistics Agency (DLA) is an agency of the DoD and serves as one of the most far-reaching agencies in supporting the U.S. Military.²⁰ DLA provides the U.S. Military with nearly 100% of its medical supplies and 84% of its spare parts.²¹ Additionally, DLA

17. See generally *DLA at a Glance*, DEF. LOGISTICS AGENCY (Oct. 29, 2012), <http://www.dla.mil/Pages/ataglance.aspx>.

18. 157 CONG. REC. S8649-50 (daily ed. Dec. 15, 2011) (statement of Sen. Sheldon Whitehouse) (remarking that the proliferation of counterfeit electronic parts throughout the defense supply chain poses a growing safety threat).

19. For example, the Defense Logistics Agency provides specific services for all branches of the military. DEF. LOGISTICS AGENCY, *supra* note 17. Conversely, the Naval Supply Systems Command provides supply chain management services only to the U.S. Navy. *Navy Supply Chain Management*, NAVY SUPPLY SYS. COMMAND (Oct. 29, 2012), <http://www.navsup.navy.mil/navsup/capabilities/nscm> [hereinafter *Navy Supply Chain Management*].

20. DEF. LOGISTICS AGENCY, *supra* note 17.

21. *Id.*

manages the reuse of military equipment across all branches of the armed services.²² The DLA uses 8 separate supply chains that manage over 5 million items to support 2100 weapons systems, acting with the size and scope of major commercial companies that provide consumer goods to the general public.²³ Conversely, the Naval Supply System Command (NAVSUP) serves a different military audience than DLA but provides many of the same services to a specific branch of the armed services, the U.S. Navy.²⁴ In managing the Navy's supply chain, NAVSUP supports the Navy's fleets by projecting procurement requirements, allocating materials, managing repairs, overseeing the lifecycle of military equipment, and ensuring the reliability of military equipment.²⁵

These agencies and others like them show the breadth of capabilities required to support the U.S. Military. But despite spending vast resources to manage the defense supply chain, agencies like DLA and NAVSUP must turn to the private sector to manufacture the goods they supply to the military.²⁶ To do this, an "original component manufacturer" (OCM) provides parts to not only DoD agencies, but also authorized and independent parts distributors who sell these parts to the DoD, prime contractors, subcontractors, and circuit board assemblers (collectively, "defense contractors").²⁷ After incorporating parts from numerous OCMs into their own products, the defense contractors eventually avail their products to DoD procurement.²⁸ This public and private partnership, however, allows counterfeit electronic parts to enter the defense supply chain, with each level of defense contractors presenting additional risks.²⁹

The worldwide production of counterfeit electronic parts has grown significantly since 2005, and the defense supply chain has felt this effect.³⁰ It is suspected that most of these counterfeits originated in

22. *Id.* Specifically, DLA operates in 48 countries and manages 26 distribution depots worldwide so that it can efficiently allocate resources to the regions of the world with higher demand for specific supplies. *Id.*

23. In 2011, DLA's sales and revenue of \$46.1 billion is greater than 90% of Fortune 500 companies. *Id.* DLA has over 27,000 employees who process over 100,000 requisitions and 11,000 contract actions per day. *Id.*

24. *See Navy Supply Chain Management, supra* note 19.

25. *Id.*

26. *See, e.g., Contracting Services, NAVY SUPPLY SYS. COMMAND* (Oct. 29, 2012), https://www.navsup.navy.mil/navsup/capabilities/contracting_service (awarding billions in annual contracts to private suppliers for the procurement of items such as the Navy's information technology).

27. *See BUREAU OF INDUS. & SEC., U.S. DEP'T OF COMMERCE, DEFENSE INDUSTRIAL BASE ASSESSMENT: COUNTERFEIT ELECTRONICS 4* (2010).

28. *Id.*

29. *See id.* at 3–4.

30. *Id.* at 170; *see also id.* at 141–64 (highlighting the specific instances of counterfeit

Asia, with more than one-third coming from China.³¹ Additionally, various sources, from large corporations to individual persons, are placing these counterfeits into the defense supply chain.³² These findings prompted both Congress and defense contractors to promulgate regulations and industry standards to fight against the proliferation of counterfeit electronic parts.³³

B. Efforts to Eliminate Counterfeit Electronic Parts

Prior to the passage of NDAA 2012, criminal counterfeit penalties addressed trafficking of counterfeit goods and services in general.³⁴ The private sector has also created industry standards for the detection of counterfeit electronic parts.³⁵ While the NDAA 2012 created criminal penalties that specifically address the trafficking of counterfeit electronic parts in scope more narrow than previous efforts,³⁶ it harmonizes the efforts of Congress and the private sector in promoting safety throughout the defense supply chain.³⁷ This Part will detail the evolution of those efforts leading up to the NDAA 2012's expansion of criminal liability for trafficking in counterfeit military goods or services.

Congress first codified criminal penalties for trafficking in counterfeit goods by passing the Trademark Counterfeiting Act of 1984.³⁸ The Act established criminal liability for "[w]hoever intentionally traffics or attempts to traffic in goods or services and knowingly uses a counterfeit mark on or in connection with such goods

electronic parts discovered in defense supply chain inventory).

31. *Id.* at 177.

32. See Bruce Rayner, *Chip Counterfeiting Case Exposes Defense Supply Chain Flaw*, ELEC. ENG'G TIMES (Oct. 23, 2011), <http://www.eetimes.com/electronics-news/4229964/Chip-counterfeiting-case-exposes-defense-supply-chain-flaw> (detailing charges against large company that knowingly sold counterfeit electronic parts); see also Thomas Claburn, *Saudi Citizen Selling Fake Cisco Gear Sentenced*, INFO. WEEK (May 7, 2010), <http://www.informationweek.com/news/security/vulnerabilities/224701177> (detailing the conviction of an individual who trafficked counterfeit electronic parts).

33. See BUREAU OF INDUS. & SEC., U.S. DEP'T OF COMMERCE, *supra* note 27, at 192. SAE AEROSPACE, SAE INT'L, SAE STANDARD AS5563, COUNTERFEIT ELECTRONIC PARTS; AVOIDANCE, DETECTION, MITIGATION, AND DISPOSITION (2009) (establishing standards for the avoidance, detection, mitigation and disposition of counterfeit electronic parts in the aerospace industry).

34. 18 U.S.C. § 2320 (2006).

35. See generally SAE AEROSPACE, SAE INT'L, *supra* note 33, at 1.

36. *But see infra* notes 55–59 and accompanying text.

37. See, e.g., Prioritizing Resources & Organization for Intellectual Property Act of 2008, Pub. L. No. 110-403, 122 Stat. 4261 (amending the most recent version of section 2320 prior to the passage of NDAA 2012, does not contain reference to any specific counterfeit good or service in which trafficking is prohibited or punished differently).

38. NDAA 2012, Pub. L. No. 98-473, § 1502(a), 98 Stat. 2178, 2178 (1984).

or services.”³⁹ The Act also provided that “[a]ll defenses, affirmative defenses, and limitations on remedies that would be applicable in an action under the Lanham Act . . . shall be applicable in a prosecution under [section 2320 of Title 18, United States Code].”⁴⁰ The only substantive amendments to section 2320 prior⁴¹ to the NDAA 2012 prohibited the trafficking of trademarked labels⁴² and the transshipment or exportation of counterfeit goods, services, or labels.⁴³ The White House advocated for an increase in those penalties,⁴⁴ and Congress echoed these concerns by expanding the penalties relating to the trafficking in counterfeit goods in section 2320.⁴⁵

The private sector has taken a different approach in addressing the volume of counterfeit electronic parts in various supply chains. For example, the International Society of Automotive Engineers (SAE), a professional organization that develops industry standards and best practices for the aerospace, automotive, and commercial-vehicles industries, proactively encourages the elimination of counterfeit electronic parts.⁴⁶ By providing uniform requirements, practices, and methods, SAE has been able to mitigate the performance, reliability, and safety risks associated with receiving and installing counterfeit electronic parts that have entered the aerospace supply chain.⁴⁷ These standards accomplish this by requiring companies to implement internal controls that address parts availability, purchasing processes, supply chain traceability, procurement contract requirements, product assurances, material controls, and reporting requirements.⁴⁸ These

39. *Id.*

40. *Id.*

41. After the NDAA 2012 amended section 2320 to create specific penalties for trafficking in counterfeit military goods and services, Congress also created specific criminal penalties for trafficking in counterfeit drugs. *See* Food and Drug Administration Safety and Innovation Act, Pub. L. No. 112-144, § 717, 126 Stat. 993, 1076–77 (2012).

42. Stop Counterfeiting in Manufactured Goods Act of 1996, Pub. L. No. 109-181, §§ 1(b), 2(b), 120 Stat. 285, 288 (2006). (prohibiting the trafficking of “labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature, knowing that a counterfeit mark has been applied thereto, the use of which is likely to cause confusion, to cause mistake, or to deceive”).

43. Prioritizing Resources & Organization for Intellectual Property Act of 2008, Pub. L. No. 110-403, § 205, 122 Stat. 4261 (“No goods or services, the trafficking in of which is prohibited by this section, shall be transshipped through or exported from the United States.”).

44. *See* EXEC. OFFICE OF THE PRESIDENT, ADMIN.’S WHITE PAPER ON INTELLECTUAL PROP. ENFORCEMENT LEG. RECOMMENDATIONS (2011) (advocating for the increase in sentences and fines for convictions of trafficking in various counterfeit goods).

45. *See* Violent Crime Control & Law Enforcement Act of 1994, Pub. L. No. 103-322, § 32014(a), 108 Stat. 2148 (2008).

46. *About SAE*, SAE INT’L (May 20, 2012), <http://www.sae.org/about/>.

47. *See* SAE AEROSPACE, SAE INT’L, *supra* note 33, at 1.

48. *See generally id.* at 2 (listing appendices that detail specific business divisions within companies that need significant oversight regarding counterfeit electronic parts).

internal controls aid defense contractors by detecting counterfeits, determining with which suppliers they should engage in business, proving conformity with buyers' specifications, and assigning liability when faced with the presence of counterfeits.⁴⁹

In order to achieve uniformity throughout the aerospace industry when confronted with a suspect part,⁵⁰ the SAE Aerospace Standards also provide standard definitions. SAE defines a "counterfeit part" as "[a] suspect part that is a copy or substitute without legal right or authority to do so or one whose material, performance, or characteristics are knowingly misrepresented by a supplier in the supply chain."⁵¹ SAE's counterfeit part definition, influenced by SAE's goal in promoting performance, reliability, and safety in parts contained throughout the aerospace supply chain, focuses on the quality of the item itself.⁵² While this definition may be suitable for the aerospace industry, it differs from the Lanham Act's definition of a "counterfeit"⁵³ and the section 2320's definition of a "counterfeit mark,"⁵⁴ which focus

49. *See id.*

50. A "suspect part" is "[a] part in which there is an indication by visual inspection, testing, or other information that it may have been misrepresented by the supplier or manufacturer and may meet the definition of counterfeit part . . ." *Id.* at 5.

51. *Id.* The Standards also provide examples of counterfeit parts, which include but are not limited to:

- a) parts which do not contain the proper internal construction (die, manufacturer, wire bonding, etc.) consistent with the ordered part; b) parts which have been used, refurbished or reclaimed, but represented as new product; c) parts which have different package style or surface plating/finish than the ordered parts; d) parts which have not successfully completed the Original Component Manufacturer's (OCM)'s full production and test flow, but are represented as completed product; e) parts sold as upscreened parts, which have not successfully completed upscreening; f) parts sold with modified labeling or markings intended to misrepresent the part's form, fit, function, or grade.

Id. Parts are not considered counterfeit if they have been refinished, upscreened, or uprated and have been identified as such. *Id.*

52. *See id.* at 1.

53. A "counterfeit" is "a spurious mark which is identical with, or substantially indistinguishable from, a register mark." 15 U.S.C. § 1127 (2006).

54. A "counterfeit mark" is

- a spurious mark—(i) that is used in connection with trafficking in any goods, services, labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature; (ii) that is identical with, or substantially indistinguishable from, a mark registered on the principal register in the United States Patent and Trademark Office and in use, whether or not the defendant knew such mark was so registered; (iii) that is applied to or used in connection

on the registered trademark instead of the quality of the underlying product. This differentiation could pose difficulties when attempting to enforce the increased penalties for trafficking in counterfeit military goods or services.

In attempting to prevent counterfeit electronic parts from entering the defense supply chain,⁵⁵ Congress amended section 2320 to establish criminal liability for those who traffic in counterfeit military goods or services.⁵⁶ Those convicted of trafficking in a specific class of counterfeit military goods or services are now subject to increased fines and penalties compared to the trafficking of other counterfeit goods, services or labels.⁵⁷ In distinguishing this specific class of penalties, section 2320 now defines a “counterfeit military good or service,” which combines the use of a counterfeit mark with good or service that does not meet military specifications or is intended for use in a military

with the goods or services for which the mark is registered with the United States Patent and Trademark Office, or is applied to or consists of a label, patch, sticker, wrapper, badge, emblem, medallion, charm, box, container, can, case, hangtag, documentation, or packaging of any type or nature that is designed, marketed, or otherwise intended to be used on or in connection with the goods or services for which the mark is registered in the United States Patent and Trademark Office; and (iv) the use of which is likely to cause confusion, to cause mistake, or to deceive; or (B) a spurious designation that is identical with, or substantially indistinguishable from, a designation as to which the remedies of the Lanham Act are made available by reason of section 220506 of title 36.

18 U.S.C. § 2320(e)(1) (2012).

55. See 157 CONG. REC. S7643 (daily ed. Nov. 17, 2011) (statement of and Sen. John McCain) (stating that the bill “will address a critically important issue we have now seen in the defense supply system with millions of counterfeit parts . . . getting into our defense system and threatening the security of our troops, the effectiveness of their mission, and costing the taxpayers a heck of a lot of money”).

56. 18 U.S.C. § 2320(a)(3):

Whoever intentionally traffics in goods or services knowing that such good or service is a counterfeit military good or service . . . the use, malfunction, or failure of which is likely to cause serious bodily injury or death, the disclosure of classified information of combat operations, or other significant harm to a combat operation . . . a member of the Armed Forces, or to national security, or attempts or conspires to violate . . . this subsection to criminal penalties.

57. *Id.* Penalties generally consisted of fines no greater than \$2,000,000 and imprisonment not more than ten years for an individual and no more than \$5,000,000 for those other than an individual. *Id.* § 2320(a)(1). The NDAA 2012 increased penalties for the specific trafficking of counterfeit military goods or services to fines not more than \$5,000,000 and imprisonment not more than twenty years for individuals and fines no greater than \$15,000,000 for those other than individuals. *Id.* § 2320(b)(3).

or national security application.⁵⁸ Section 2320 still allows defendants subject to criminal prosecution for the trafficking in counterfeit military goods or services to assert Lanham Act defenses, affirmative defenses, and limitations on remedies.⁵⁹

As opposed to the reactive nature of criminal penalties, the remainder of section 818 attempts to proactively prevent counterfeit electronic parts from entering the defense supply chain.⁶⁰ To address the detection and avoidance of counterfeit electronic parts, the NDAA 2012 requires the Secretary of Defense to implement internal controls with the DoD and to revise the DoD Supplement to the Federal Acquisition Regulations related to the procurement of counterfeit electronic parts.⁶¹ The internal controls will define the terms “counterfeit electronic part” and “suspect counterfeit electronic part;”⁶² require personnel training regarding counterfeit electronic parts; implement procedures for the inspecting, testing, reporting and quarantining of counterfeit electronic parts; and create guidelines and remedial actions for suppliers who fail to detect and avoid counterfeit electronic parts.⁶³ The revisions to the Federal Acquisition Regulations will assign the responsibility of detecting and avoiding counterfeit electronic parts to defense contractors; require that all defense contractors obtain electronic parts only from original manufacturers, trusted suppliers,⁶⁴ and authorized dealers; and establish procedures for contractors to report the detection

58. *Id.* § 2320(e)(4):

(4) The term ‘counterfeit military good or service’ means a good or service that uses a counterfeit mark on or in connection with such good or service and that—(A) is falsely identified or labeled as meeting military specifications, or (B) is intended for use in a military or national security application.

59. *Id.* § 2320(d).

60. 157 CONG. REC. S7647–48 (daily ed. Nov. 17, 2011) (statement of Sen. Carl Levin) (describing the reasons for which proactive measures are needed to prevent counterfeit electronic parts from entering the defense supply chain).

61. NDAA 2012, Pub. L. No. 112-81, § 818(b)–(c), 125 Stat. 1298, 1493–96 (2012). These actions will be based on an internal assessment of the DoD’s current acquisition policies and systems. *Id.* § 818(a), 125 Stat. at 1493.

62. The DoD gave a preliminary indication of how counterfeit material would be defined in these preventions programs. See Kendall, Overarching DoD Counterfeit Prevention Guidance, *supra* note 12, at 1 (defining “counterfeit material” as “an item that is an unauthorized copy or substitute that has been identified, marked and/or altered by a source other than the item’s legally authorized source and has been misrepresented to be an authorized item of the legally authorized source” and suggesting that “a used item represented as a new item may also be subject to fraudulent representation procedures”).

63. NDAA 2012, § 818(b), 125 Stat. at 1493–94.

64. *Id.* § 818(c)(3), 125 Stat. at 1495 (creating a trusted supplier program to reduce the risk of unsafe electronic parts from reaching contractors further down the supply chain).

of counterfeit electronic parts.⁶⁵ Additionally, the Secretary of Defense will establish training programs to assist contractors with their new responsibilities pertaining to the detection and avoidance of counterfeit electronic parts.⁶⁶ And since a majority of these counterfeit electronic parts enter the defense supply chain from overseas,⁶⁷ the Department of Homeland Security will also establish procedures for inspecting electronic parts imported from other countries.⁶⁸

Congress defined the amendment's scope as applying to "electronic parts," which are defined in section 818 as "an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly."⁶⁹ This is one of the various definitions related to counterfeit electronic parts and counterfeit military goods or services contained in section 818 or section 2320, all of which refer to different regulations or codes that Congress has enacted to promote safety and reduce risk associated with the defense supply chain.⁷⁰ However, the inconsistent use of terms throughout both public and private prevention measures and criminal penalties⁷¹ will cause confusion and difficulty for the DoD in implementing, and defense contractors in adhering to, the section 818 regulations, which could interfere with Congress's goal of creating a safe defense supply chain.⁷²

There are two ways to approach the solution for counterfeit electronic parts—creating liability for the improper use of the registered trademark itself, or for failing to produce the electronic part with

65. *Id.* § 818(c), 125 Stat. at 1494–96.

66. *See id.* § 818(e), 125 Stat. at 1496.

67. *See* BUREAU OF INDUS. & SEC., U.S. DEP'T OF COMMERCE, *supra* note 27, at 170.

68. NDAA 2012, § 818(d), 125 Stat. at 1496.

69. *Id.* § 818(g)(2), 125 Stat. at 1496–97.

70. *See* 157 CONG. REC. S7647–48 (daily ed. Nov. 17, 2011) (statement of Sen. Carl Levin) (describing the reasons for which proactive measures are needed to prevent counterfeit electronic parts from entering the defense supply chain).

71. *See, e.g.*, 15 U.S.C. § 1127 (2006) (defining "counterfeit"); *id.* § 1116(d)(1)(B) (defining "counterfeit mark"); 18 U.S.C. § 2320(f)(1) (defining "counterfeit mark"); *id.* § 2320(f)(4) (defining "counterfeit military good or service"); NDAA 2012, § 818(f)(2), 125 Stat. at 1298 (defining "electronic part"); *id.* § 818(b)(1) (requiring the Secretary to establish definitions of "counterfeit electronic part" and "suspect counterfeit electronic part"); Kendall, Overarching DoD Counterfeit Prevention Guidance, *supra* note 12, at 1; Kendall, DoD Supply Chain Material Management Policy, *supra* note 12, at 16–19 (defining "counterfeit material" and "suspect counterfeit"); SAE AEROSPACE, SAE INT'L, *supra* note 33, at 5 (defining "counterfeit part" and "suspect part"); S. COMM. ON ARMED SERV., INQUIRY INTO COUNTERFEIT ELEC. PARTS IN THE DEP'T OF DEF. SUPPLY CHAIN, S. REP. NO. 112-167, at 36–37 (2012) (defining "counterfeit").

72. *See* Metzger, *supra* note 15, at 3 (suggesting that the confusion over the "counterfeit" definition could draw controversy when interpreting the section 818 regulations, thus encouraging contractors to implement overly stringent testing and inspection procedures).

sufficient standards of quality. In order to best prevent counterfeit electronic parts from entering the defense supply chain, the Secretary of Defense should narrowly focus on the quality of the good. The Lanham Act's trademark principles are not the best means to assure the uniform compliance in accomplishing Congress's goals in enacting section 818.

III. LANHAM ACT APPLICATION TO COUNTERFEIT MARKS

The nature of the defense supply chain presents distinct issues compared to other typical counterfeit cases. The various levels of defense contractors, subcontractors, and suppliers involved with DoD procurement each present an additional opportunity for counterfeit electronic parts to enter the defense supply chain.⁷³ While the inclusion of proactive detection programs in the section 818 highlight the importance of removing counterfeits electronic parts before they enter the final product, it will be difficult to hold the producers of these counterfeits accountable because so many are located overseas.⁷⁴ Despite section 2320's increased penalties, the statute's reliance on the Lanham Act does not provide adequate reactive measures for achieving Congress and the White House's goal of punishing those who allow counterfeit electronic parts to enter the defense supply chain.⁷⁵ This Part will discuss the Lanham Act's impact on Congress's goal of making a safer defense supply chain.

The Lanham Act's prohibition against the use of counterfeit marks provides a civil cause of action to owners of registered trademarks against any person who uses in commerce a reproduction or copy of the registrant's mark "in connection with the sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive."⁷⁶ The remedies available to the registrant, however, are limited to an injunction when the infringer's acts are committed without "knowledge that such imitation is intended to be used to cause confusion, or to cause mistake, or to deceive."⁷⁷ The knowledge requirement is similar to section 2320 because the offense requires the intent to traffic in counterfeit military goods or services.⁷⁸ Section 2320 also provides various affirmative defenses which are based on the

73. See BUREAU OF INDUS. & SEC., U.S. DEP'T OF COMMERCE, *supra* note 27, at 3-4.

74. See *id.*

75. See *supra* notes 44-45 and accompanying text.

76. 15 U.S.C. § 1114(1)(a).

77. *Id.* § 1114(1). If the infringer acted with knowledge, the registrant can recover profits or damages. *Id.*

78. 18 U.S.C. § 2320(a)(3) (2012).

defenses available to infringers of the Lanham Act.⁷⁹ However, these sections differ due to the various “counterfeit” definitions contained throughout both sections, especially in regard to counterfeit military goods or services.

The Lanham Act defines a “counterfeit” as a “spurious mark which is identical with, or substantially indistinguishable from, a registered mark.”⁸⁰ This definition is one of four requirements for a “counterfeit mark” to be considered a “spurious mark” under section 2320; the mark must also be used in connection with trafficking in any goods or services and applied to or used in connection with the goods or services for which the mark is registered, and the use of the mark must also be likely to cause confusion, to cause mistake, or to deceive.⁸¹ However, the Lanham Act’s definition of a “counterfeit mark” differs from section 2320.⁸² Section 2320’s additional requirement for a “counterfeit military good or service” requires that the “counterfeit mark,” “be used on or in connection with such good or service that is falsely identified as meeting military specifications, or is intended for use in a military or national security application.”⁸³ The elements of the criminal offense require that the defendant have intentionally used a counterfeit mark in connection with the goods or services,⁸⁴ but this statute has yet to be analyzed with regard to counterfeit military goods or services.

Section 2320’s knowledge requirement related to the use of a “counterfeit mark” has been extended beyond the use of spurious marks. In *United States v. Petrosian*,⁸⁵ the Ninth Circuit held that section 2320 applied to the defendant’s resale of genuine Coca-Cola bottles which defendant refilled with a cola-like carbonated beverage that defendant knew was not Coca-Cola.⁸⁶ The court reasoned that “[w]hen a genuine trademark is affixed to a counterfeit product, it becomes a spurious mark” since “[a] ‘spurious’ mark is one that is false or inauthentic.”⁸⁷ Under this analysis, the court expands the definition of “counterfeit

79. *Id.* § 2320(d).

80. 15 U.S.C. § 1127.

81. 18 U.S.C. § 2320(f)(1).

82. 15 U.S.C. § 1116(d)(1)(B)(i):

[A] counterfeit of a mark that is registered on the principal register in the United States Patent and Trademark Office for such goods or services sold, offered for sale, or distributed and that is in use, whether or not the person against whom relief is sought knew such mark was so registered.

83. 18 U.S.C. § 2320(f)(4).

84. *See United States v. Baker*, 807 F.2d 427 (5th Cir. 1986).

85. 126 F.3d 1232 (9th Cir. 1997).

86. *Id.* at 1233.

87. *Id.* at 1234.

mark” under section 2320 to include genuine marks attached to inferior products. The court relies on the Lanham Act’s “counterfeit mark” definition in its analysis, along with other cases in which courts have held “defendants civilly liable under the Lanham Act for affixing genuine marks to counterfeit products.”⁸⁸

While section 2320 has yet to be applied to counterfeit military goods or services, there are similar instances relevant to counterfeit electronic parts where both contractors and subcontracts used counterfeit parts in the manufacturing of the final product. In *United States v. Brooks*,⁸⁹ defendants operated a marine electrical supply business which sold electrical parts and custom-assembled electrical components to both civilian and military customers.⁹⁰ Defendants were charged with violating section 2320 by delivering to the U.S. Navy both components containing trademarks of approved military suppliers which defendants actually assembled and parts which defendant rebuilt but represented to the client as new.⁹¹ The Fourth Circuit rejected defendant’s argument that inclusion of defendant’s interior labels on custom-assembled components absolves them of liability for placing counterfeit marks on the exterior of the component.⁹² The Fourth Circuit reasoned that defendants’ intentional use of a false mark on the custom-assembled electrical components that contained used parts, the use of which was likely to cause confusion, was sufficient to hold defendants liable for counterfeiting under section 2320.⁹³

The reasoning provided in the *Petrosian* and *Brooks* gives helpful insight regarding the Lanham Act application to counterfeit military goods and services. Both cases focused on trademark infringers intentionally using another’s genuine trademark on counterfeit or refurbished products. While those cases show that one may be held liable for using another’s registered trademark with counterfeit goods, manufacturers in the defense supply chain are using their own genuine trademarks on electronic parts. Section 818 attempts to address a manufacturer’s use of counterfeit components in electronic parts,⁹⁴ but the inclusion of this provision in criminal statutes is problematic.

88. *Id.* (citing *Westinghouse Elec. Corp. v. Gen. Circuit Breaker & Elec. Supply, Inc.*, 106 F.3d 894, 899–900 (9th Cir. 1997); *Gen. Elec. Co. v. Speicher*, 877 F.2d 531, 534 (7th Cir. 1989)).

89. 111 F.3d 365 (4th Cir. 1997).

90. *Id.* at 367–68. Defendants often assembled these electrical components with used parts. *Id.* at 368.

91. *Id.* at 368.

92. *Id.* at 372.

93. *Id.*

94. See 157 CONG. REC. S7647 (daily ed. Nov. 17, 2011) (statement of Sen. John McCain) (regarding amendment 1092 to the NDAA 2012); S. COMM. ON ARMED SERV., *supra* note 71, at 228–39.

The language of section 2320(a)(3) contains two separate knowledge requirements. One must “intentionally [traffic] in goods or services,” and one must also “[know] that such good or service is a counterfeit military good or service.”⁹⁵ Unlike *Petrosian* and *Brooks*, in which defendants knew the products they sold were counterfeit products,⁹⁶ defense contractors often are unaware that counterfeit electronic parts exist in their products.⁹⁷ Additionally, defendants may raise the Lanham Act defense that they have received consent to use a counterfeit mark.⁹⁸ Therefore, section 2320 would not hold these parties criminally liable for counterfeiting. Section 818 does increase requirements for defense contractors in the testing and detecting of counterfeit electronic parts,⁹⁹ but it is nearly impossible for manufactures to ensure that every single electronic part that they produce will be free from counterfeits.¹⁰⁰ Moreover, because manufacturers often receive these counterfeit electronic parts from foreign producers,¹⁰¹ this leads to a situation where the United States will not be able to enforce section 2320 amendments

95. 18 U.S.C. § 2320(a)(3) (2012).

96. See *United States v. Petrosian*, 126 F.3d 1232, 1233 (9th Cir. 1997); *Brooks*, 111 F.3d at 368.

97. See BUREAU OF INDUS. & SEC., U.S. DEP’T OF COMMERCE, *supra* note 27, at 5–6.

98. 15 U.S.C. § 1115(1)(a) (2006) (“any person who shall, without the consent of the registrant—use in commerce any . . . counterfeit . . . of a registered mark in connection with the . . . sale of any goods or services on or in connection with which such use is likely to cause confusion, mislead, or to deceive”). While the argument that the owner of a registered mark gives consent to itself to use its own mark may seem obvious, it is still an available defense since section 2320 provides that “all defenses, affirmative defenses, and limitations on remedies that would be applicable in an action under the Lanham Act shall be applicable in a prosecution under this section.” 18 U.S.C. § 2320(d). Furthermore, the Lanham Act’s definition of a “counterfeit mark” specifically excludes

any mark or designation used on or in connection with goods or services of which the manufacture or producer was, at the time of the manufacture or production in question authorized to use the mark or designation for the type of goods or services so manufactured or produced, by the holder of the right to use such mark of designation.

15 § U.S.C. 1116(d)(1)(B).

99. NDAA 2012, Pub. L. No. 112-81, § 818(b)–(c), 125 Stat. 1298, 1493–96 (2012).

100. While section 818 places the cost of reworking and correcting counterfeit electronic parts and suspect counterfeit electronic parts on contractors, *id.* § 818(c)(2)(B), 125 Stat. at 1494–95, Congress has proposed an amendment to section 818 relieving defense contractors of this cost if the defense contractor has properly implemented and complied with a counterfeit detection and avoidance program, procured the parts from a trusted supplier, and promptly notified the Government. See National Defense Authorization Act for Fiscal Year 2013, H.R. 4310, 112th Cong. § 816 (2012). *But see* National Defense Authorization Act for Fiscal Year 2013, S. 3524, 112th Cong. (2012) (removing the House amendment related to safe harboring costs from section 818).

101. See BUREAU OF INDUS. & SEC., U.S. DEP’T OF COMMERCE, *supra* note 27, at 170.

and impose increased penalties for entering counterfeit electronic parts into the defense supply chain because of section 2320's knowledge requirement and Lanham Act defenses.

IV. ALTERNATIVE MEANS FOR ACHIEVING NDAA 2012'S INTENDED PURPOSE

While section 2320's increased penalties do not adequately address Congress's goal of preventing counterfeit electronic parts from entering into the defense supply chain, there are alternative methods for achieving this goal. While suspension or disbarment from DoD procurement may dissuade some defense contractors from violating the new provisions,¹⁰² this Part will propose alternative methods for preventing counterfeit electronic parts from entering the defense supply chain. Specifically, this Part will focus on section 818's yet to be codified rules regarding contractor responsibilities for counterfeit electronic parts.¹⁰³

Section 818's yet-to-be-promulgated measures addressing counterfeit electronic parts provide proactive means that the Secretary of Defense can use to supplement the Lanham Act's shortcomings. Section 818 requires the Secretary of Defense to promulgate new regulations concerning the impact of counterfeit electronic parts currently in the defense supply chain, proper training for those throughout the defense supply chain on how to properly detect counterfeit electronic parts, processes for responding to the detection of counterfeit electronic parts, and remedial measures for defense contractor's failure to comply with regulations.¹⁰⁴ To accomplish these goals, the regulations require defense contractors to implement programs that enhance detection and avoidance of counterfeit electronic parts.¹⁰⁵ The detection programs can supplement the failures of section

102. See NDAA 2012, § 818(c)(3), 125 Stat. at 1495.

103. See *supra* notes 60–66 and accompanying text.

104. See NDAA 2012, § 818(c)(2)–(5), 125 Stat. at 1298.

105. *Id.* § 818(e), 125 Stat. at 1494–96. Covered contractors must implement policies and procedures that

[a]ddress--(i) the training of personnel; (ii) the inspection and testing of electronic parts; (iii) processes to abolish counterfeit parts proliferation; (iv) mechanisms to enable traceability of parts; (v) use of trusted suppliers; (vi) the reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts; (vii) methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit; (viii) the design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts; and (ix) the flow down of counterfeit avoidance and detection requirements to

2320 by creating alternative methods for holding defense liable in their selection of suppliers. Additionally, these programs could help establish a defense contractor's knowledge of using electronic parts of substandard quality or insufficient inspection procedures in the event of bringing sanctions.

A. Clarifying the "Counterfeit" Definition

For the DoD regulations to adequately satisfy Congress's intended effect of promoting safety throughout the defense supply chain,¹⁰⁶ the definitions related to "counterfeit electronic part" must avoid section 2320's shortcomings.¹⁰⁷ The definitions should be consistently applied throughout all contractor and department regulations.¹⁰⁸ The Secretary should consider all aspects of Congress's goals and the impact that inconsistent definitions or regulations could have on the defense contracting industry when defining the scope of these regulations.¹⁰⁹

Specifically, the definitions contained in the new regulations should avoid reference to the Lanham Act. Reliance on Lanham Act definitions and principles allows contractors to assert one of the Act's numerous knowledge-related defenses, thus making it more difficult for the DoD to hold contractors liable for the use of counterfeit electronic parts.¹¹⁰ This does not align with Congress's concern of ensuring quality electronic parts are present throughout the defense supply chain.¹¹¹ Instead of relying on the term "counterfeit," the regulations could include other terms that still address the underlying quality of the good.¹¹²

subcontractors; and (B) establish processes for the review and approval of contract systems

Id.

106. See *supra* text accompanying notes 55, 60.

107. See NDAA 2012, § 818(b)(1), 125 Stat. at 1493–94. The definitions will also include "previously used parts represented as new." *Id.*

108. See *supra* note 71 and accompanying text.

109. NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2013, H.R. REP. NO. 112-479, at 186 (2012) (suggesting "continuing communication between industry and policy makers to be instrumental to effecting sound policies and policies . . . in mitigating the treatment of counterfeit electronic parts").

110. 18 U.S.C. § 2320(d) (2012).

111. See *supra* text accompanying note 55, 60.

112. Other regulations in the Defense Acquisition Regulations System use terms other than "counterfeit" that address the underlying quality of a contractor's product. See, e.g., Federal Acquisition Regulations System, 48 C.F.R. § 252.244-7001(a) (2011) (using the term "significant deficiency" to define a shortcoming in a contractor purchasing system); *id.* § 253.209-1(a)(i)(C) (requiring review of contractor's "quality assurance" capabilities); *id.* § 252.246-7003(a) (using "critical safety item" to apply to all aspects of a contractor system

The Defense Secretary should ensure that these inspection and testing regulations broadly apply to all aspects underlying the quality of the electronic parts. For example, Congress specifically identified the operating conditions and longevity of electronic parts as particular areas of concern which could easily be overlooked if not properly addressed by DoD.¹¹³ The current “counterfeit” definitions promulgated since Congress passed section 818 address items that do not meet military specifications¹¹⁴ and items that are unauthorized copies or substitutes that have been illegally altered and misrepresented as produced by the legally authorized source.¹¹⁵ To adequately address Congress’s concerns of electronic parts performing under adequate conditions and for specified periods of time, DoD regulations related to testing should include these factors in any future definition related to the quality of the electronic part.¹¹⁶ Also, development of proper testing requirements will require cooperation between DoD and defense contractors to ensure that specifications for each electronic part are defined ahead of time.¹¹⁷ Cooperation will prevent substandard parts from entering the defense supply before they can cause harm and relieve DoD from relying on inadequate criminal remedies under section 2320.

In addition to the testing and inspection requirements, the DoD’s focus on “critical items” in its internal guidance for implementing counterfeit prevention measures raises a question whether the regulations will require contractors to notify the DoD of only a subset of electronic parts that would exclude other electronic parts whose substandard quality would still impact safety of products in the defense supply chain.¹¹⁸ Instead, contractor notification requirements should

which could have a safety impact). In fact, the section 818 requires that the “processes for the review and approval of contractor systems for the detection and avoidance of counterfeit and suspect counterfeit electronic parts” should be comparable to the processes established for contractor business systems, as described above in part 252.244-7001(a). NDAA 2012, § 818(e)(2)(B), 125 Stat. at 1496.

113. S. COMM. ON ARMED SERV., *supra* note 71, at 36–37; *see also* Metzger, *supra* note 15, at 6.

114. 18 U.S.C. § 2320(f)(4)(A) (defining “counterfeit military good or service”).

115. Kendall, *Overarching DoD Counterfeit Prevention Guidance*, *supra* note 12, at 1 (defining “counterfeit material”).

116. The DoD has already implied that these considerations may not be addressed in the detection and inspection regulations. *See* PAUL D. PETERS, DEPARTMENT OF DEFENSE, ANTI-COUNTERFEIT PRODUCT SUPPORT MANAGERS CONFERENCE 8 (June 6, 2012) (stating that inspections will require electronic parts to perform according to all required specifications, but omitting longevity of performance and performance under strenuous conditions as inspection requirements when other specific inspection and test processes are listed).

117. Metzger, *supra* note 15, at 8.

118. Kendall, *Overarching DoD Counterfeit Prevention Guidance*, *supra* note 12, at 1; *see also* Metzger, *supra* note 15, at 3.

parallel the testing and detection requirements for electronic parts.¹¹⁹ Broader application of the notification requirement will avoid confusion and inconsistent application of the regulations and help improve the safety of products in the defense supply chain.¹²⁰

The Secretary of Defense can look to other industry standards, such as those provided by SAE as guidance in its rule promulgation.¹²¹ Additionally, the Secretary could look to alternative definitions contained in the Defense Acquisition Regulation System to avoid the “counterfeit” confusion altogether.¹²² Congress and the defense contracting industry have similar goals in improving the quality of their products by eliminating counterfeit electronic parts, so SAE standards would be helpful in defining terms and regulations that are consistent with Congress’s intent in passing the NDAA 2012. Failure to create consistent definitions will lead to ambiguous interpretations and differing applications, as has been seen throughout various federal courts of appeal¹²³ and suggested in commentary analyzing section 818.¹²⁴

119. Metzger suggests that Kendall’s memorandum addresses the detection and inspection of more than just electronic parts. Metzger, *supra* note 15, at 2. While discussion of non-electronic parts is beyond the scope of this Note, the DoD should consider the implications that the section 818 regulations would have on other existing or future detection and testing requirements. See DEP’T OF DEF., OPEN FAR CASES 2 (Oct. 26, 2012), available at <http://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf> (suggesting that portions of section 818 will be applied to Federal Acquisition Regulations, not just the Defense Federal Acquisition Regulations, and using the term “non-conforming supplies” rather than “counterfeits” in case number 2013-002).

120. The memorandum indirectly refers to “critical safety items” as defined in part 252.246-7003(a) in relation to contractor purchasing systems. Kendall, Overarching DoD Counterfeit Prevention Guidance, *supra* note 12, at 2. The term “critical safety item” would seem to encompass all electronic parts which could have a safety impact, see 48 C.F.R. § 252.246-7003(a), but the terms should be used consistently to avoid confusion.

121. See generally SAE AEROSPACE, SAE INT’L, *supra* note 33, at 5. See also Metzger, *supra* note 15, at 3 (noting the Senate’s favorable treatment of SAE AS5553-2009); CRAIG HOLMAN ET AL., FEATURE COMMENT: PREPARING FOR NEW RULES TO COMBAT COUNTERFEIT PARTS, 54 No. 23 Gov’t Contractor ¶ 189 (suggesting that contractors who do not have an existing counterfeit mitigation plan should adopt existing roadmaps, such as the SAE Aerospace guidelines, to prevent counterfeits from entering the defense supply chain).

122. See *supra* note 71 and accompanying text.

123. Compare *United States v. Petrosian*, 126 F.3d 1232, 1234 (9th Cir. 1997) (indicating that the “counterfeit” definition in section 2320 is identical to that application in the Lanham Act), with *United States v. Hanafy*, 302 F.3d 485 (5th Cir. 2002) (rejecting the 9th Circuit’s indication from *Petrosian* because of the criminal and civil distinction between section 2320 and the Lanham Act) (citing *United States v. Giles*, 213 F.3d 1247, 1250 (10th Cir. 2000)).

124. See Metzger, *supra* note 15, at 2.

B. *Alternative Sources of Liability*

Despite section 2320's shortcomings in relying upon trademark principles to create criminal liability for defense contractors who allow counterfeit electronic parts to enter the defense supply chain, the yet-to-be promulgated contractor responsibilities¹²⁵ may allow DoD to hold contractors liable based on other fraud-based statutes. For example, the United States can charge defense contractors with violating the Federal False Claims Act¹²⁶ (FCA) for knowingly¹²⁷ submitting false or fraudulent claims¹²⁸ to the United States for payment or approval. Since the FCA is a civil statute, the United States may be more successful in bringing actions under the FCA rather than section 2320 while still adhering to Congress's goals of increased penalties for use of counterfeit electronic parts.

A defense contractor violates the FCA if it withholds information about its noncompliance with material¹²⁹ contractual requirements.¹³⁰

125. See NDAA 2012, Pub. L. No. 112-81, § 818(e)(2)(A), 125 Stat. 1298, 1496 (2012).

126. 31 U.S.C. §§ 3279–3733 (2012).

127.

The terms “knowing” and “knowingly” – mean that a person, with respect to information – has actual knowledge of the information; acts in deliberate ignorance of the truth or falsity of the information; or acts in reckless disregard of the truth or falsity of the information; and require no proof of specific intent to defraud.

Id. § 3729(b)(1).

128.

The term “claim” means any request or demand, whether under contract or otherwise, for money or property and whether or not the United States has title to the money or property, that – is presented to an officer, employee, or agent of the United States; or is made to a contractor, grantee, or other recipient, if the money or property is to be spent or used on the Government's behalf or to advance a Government program or interest, and if the United States Government – provides or has provided any portion of the money or property requested or demanded; or will reimburse such contractor, grantee, or other recipient for any portion of the money or property which is requested or demanded.

Id. § 3729(b)(2)(A). “The term ‘claim’ . . . does not include requests or demands for money or property that the Government has paid to an individual as compensation for Federal employment or as an income subsidy with no restrictions on that individual's use of the money or property.” *Id.* § 3729(b)(2)(B).

129. “The term ‘material’ means having a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property.” *Id.* § 3729(b)(4). “The existence of express contractual language specifically linking compliance to eligibility for payment may well constitute dispositive evidence of materiality, but it is not . . . a necessary condition.” United

While the federal circuits disagree as to whether such false certifications require a condition precedent,¹³¹ the DoD can avoid this problem by clearly drafting the new regulations required by section 818. Those regulations should require all contractual arrangements between the United States and defense contractors to contain a provision that expressly requires defenses contractors, as a condition of payment on each submission to United States, to certify that it complied with all inspection and testing requirements under the new section 818 regulations.

Unlike section 2320, a defense contractor is not required to have specific intent to violate the FCA.¹³² Rather, in establishing knowledge under the FCA based on the theory of implied certification, “the FCA requires the plaintiff to prove that the defendant knows (1) that it violated a contractual obligation, and (2) that its compliance with the obligation was material to the government’s decision to pay.”¹³³ In assessing whether government contractors violated the FCA by submitting claims to the United States for payment related to products of substandard quality, courts will examine whether the contractor was aware, or should have been aware, that the product was not what the contractor purported it to be.¹³⁴ Additionally, defense contractors will not be able to assert Lanham Act defenses which are available under section 2320.¹³⁵

Most uniquely, the FCA undermines a contractor’s attempts to conceal its noncompliance with onerous testing and inspection procedures by encouraging private individuals to report fraud by defense contractors.¹³⁶ If a whistleblower brings a successful action

States v. *Sci. Applications Intern. Corp.*, 626 F.3d 1257, 1269 (D.C. Cir. 2010). Materiality may also be established through “testimony demonstrating that parties to the contract understood that the payment was conditional on compliance with the requirement at issue.” *Id.*

130. *Sci. Applications Intern. Corp.*, 626 F.3d at 1269. Often, contractual requirements may require the contractor to expressly certify that the contractor inspected and tested the quality of the goods before submitting the goods to the United States. *See, e.g.*, *United States v. Advance Tool Co.*, 902 F. Supp. 1011, 1016 (W.D. Mo 1995), *aff’d*, 86 F.3d 1159 (8th Cir. 1996) (requiring contractor to perform all inspections and tests necessary to determine that the goods conformed to contract specifications).

131. *Compare Sci. Applications Intern. Corp.*, 626 F.3d at 1269–70 (allowing the United States to recover for a violation of a condition that was not an express prerequisite to payment), *with Mikes v. Straus*, 274 F.3d 687, 697–700 (2d Cir. 2001) (allowing the United States to recover, absent express contractual terms, only when the underlying statute or regulation upon the plaintiff relies expressly states that the defendant must comply in order to be paid).

132. *Advance Tool Co.*, 902 F. Supp. at 1016.

133. *Sci. Applications Intern. Corp.*, 626 F.3d at 1271.

134. *Crane Helicopter Serv., Inc. v. United States*, 45 Fed. Cl. 410, 435–36 (1999).

135. *See* 18 U.S.C. § 2320(d) (2012) (allowing defendant to assert any defenses available under the Lanham Act when charged with violations of section 2320).

136. 31 U.S.C. § 3730(b)(1) (2012) (“A person may bring a civil action for a violation of

under the FCA, the whistleblower receives an award equal to a percentage of the funds recovered by the United States in the action.¹³⁷ Since the FCA increases the likelihood that the United States will discover a contractor's noncompliance with section 818's testing and inspection requirements, the FCA complements Congress's goal of preventing counterfeit electronic parts from entering the defense supply chain.

Because the forthcoming regulations described in section 818 will require defense contractors to inspect and test electronic parts, the FCA may allow the United States to recover considerable funds if contractors fail to comply with these new regulations.¹³⁸ FCA violators are liable to the United States for 3 times the amount of damages which the United States sustains because of defendant's false claims,¹³⁹ a civil penalty of \$5,000 to \$10,000 for each false claim that defendant submits to the government,¹⁴⁰ and reasonable expenses, attorneys' fees, and costs.¹⁴¹ While on its face the recovery available to the United States under the FCA may not seem as substantial as the criminal penalties under section 2320,¹⁴² damages and civil penalties under the FCA are easier to obtain.¹⁴³

Compared to section 2320, the FCA serves as a better avenue to

section 3729 for the person and for the United States Government").

137. *Id.* § 3730(d) (awarding the whistleblower, depending on the circumstances articulated in subsection 3730(d), anywhere between 15% and 30% of the proceeds of the action or settlement of the claim).

138. *See, e.g.,* *United States v. Advance Tool Co.*, 902 F. Supp. 1011, 1016 (W.D. Mo 1995) (finding defendant knowingly submitted false claims within the meaning of the FCA because defendant was required under contract to inspect and test the products to determine that the products conformed with the contract requirements).

139. 31 U.S.C. § 3729(a). Specifically, actual damages under the FCA are equal to the market value of the products the government sought under the contract minus the market value of the products the government received and retained from the defendant. *United States v. Bornstein*, 423 U.S. 303, 316 n.13 (1976).

140. 31 U.S.C. § 3729(a). *See also, e.g.,* *United States v. Rule Indus., Inc.*, 878 F.2d 535, 538 (1st Cir. 1989) (assessing a total of 302 civil penalties for defendant's false claim on each of the 302 invoices which defendant submitted to the government for payment during a two year period). Additionally, civil penalties are recoverable under the FCA even if the United States fails to show actual damages; *see United States ex rel. Hagood v. Sonoma Cnty. Water Agency*, 929 F.2d 1416, 1421 (9th Cir. 1991) (citing *Rex Trailer Co. v. United States*, 350 U.S. 148, 153 n.5 (1956)).

141. 31 U.S.C. § 3730(d)(1)–(2) (awarding successful *qui tam* plaintiffs "reasonable expenses which the court finds to have been necessarily incurred, plus reasonable attorneys' fees and costs").

142. First time violations for knowingly trafficking in counterfeit military goods or services can result in fines up to \$5,000,000 for individuals and \$15,000,000 for organizations. 18 U.S.C. § 2320(b)(3)(A) (2012). Second or subsequent violations can result in fines up to \$15,000,000 for individuals and \$30,000,000 for organizations. *Id.* § 2320(b)(3)(B).

143. *See supra* notes 130–38 and accompanying text.

achieving Congress's ultimate goal in passing the NDAA 2012: safety.¹⁴⁴ If section 818 regulations will require that defense contractors certify their compliance with their testing and inspection responsibilities, the United States may be able to bring FCA actions against defense contractors. This would encourage defense contractors to comply with the NDAA's testing and inspection provisions, reducing the chance that counterfeit electronic parts enter the defense supply chain in the first place. Without the certification requirement and potential FCA liability, contractors would have no incentive for notifying the government that the contractor, upon later discovery, unknowingly submitted counterfeit electronic parts to the defense supply chain. Additionally, the FCA's encouragement of whistleblower participation in bringing actions against defense contractors addresses other goals sought by the NDAA, such as aiding DoD investigations of suspected counterfeit electronic parts by providing first-hand information of potential violations.¹⁴⁵ Conversely, defense contractors can only be held criminally liable under section 2320 if they intentionally supply the government with military goods or services which the contractor knows are counterfeit military goods or services.¹⁴⁶ The Defense Secretary should carefully consider these alternatives when promulgating the section 818 rules.

V. CONCLUSION

Unfortunately, the problem with this definition is likely to continue due to the NDAA 2012's use of the word "counterfeit" in describing the "electronic parts" with which Congress was concerned in preventing from entering the defense supply chain.¹⁴⁷ As evidenced by the use of the term "counterfeit," congressional members have assumed that reliance on the Lanham Act's trademark principles is the best method for preventing these counterfeit electronic parts from entering the defense supply chain.¹⁴⁸ But because Congress is more concerned with the quality of the underlying good, alternatives to relying on trademark

144. See *supra* notes 55, 60 and accompanying text.

145. See Metzger, *supra* note 15, at 4.

146. 18 U.S.C. § 2320(a)(3).

147. See NDAA 2012, Pub. L. No. 112-81, § 818, 125 Stat. 1298 (2012) (titled "Detection and Avoidance of Counterfeit Electronic Parts").

148. Although no congressional support for section 818 of the NDAA 2012 includes use of the terms "Lanham Act" or "Trademark," Congress's reliance on the Lanham Act is evidenced by such use in the bill itself. See 18 U.S.C. § 2320(d) (allowing Lanham Act defenses). The Department of Commerce assessment of counterfeit electronic parts in the defense supply chain also uses the term "counterfeit" throughout its analysis. See BUREAU OF INDUS. & SEC., U.S. DEP'T OF COMMERCE, *supra* note 27, at 192.

and counterfeit principles would better serve Congress's goal of ensuring the quality of electronic parts throughout the defense supply chain.¹⁴⁹

149. Section 2320's definition of "counterfeit military good or service" further evidences Congress's concern with the underlying quality of the good by specifically identifying goods or services that fail to meet military specifications. 18 § U.S.C. 2320(e)(4).