ENCRYPTION: WHAT IS A DEFENSE CONTRACTOR'S ROLE IN A CYBER WORLD?

Brandon M. Basso*

I. Introduction

Before the twenty-first century, warfare consisted more of artillery than computer network attacks,[1] yet, the increase in both terrorist activity and number of cyber warriors prompted Congress to introduce legislation to address the evolving cyber threat.[2] In 2002, the implementation of the SAFETY Act started the production of high

*J.D. Candidate, Suffolk University Law School, 2018.

[1] *See* Dieter Storz, *Artillery*, INTERNATIONAL ENCYCLOPEDIA OF THE FIRST WORLD WAR (Mar. 8, 2016), *archived at* https://perma.cc/RH6G-3TCQ (explaining that artillery was primarily used for mobile warfare until 1914).

[2] *See* William Banks, *The Role of Counterterrorism Law in Shaping Ad Bellum Norms for Cyber Warfare*, 89 INT'L L. STUD. 157, 180-82 (2013) (noting the necessity to develop counterterrorism and cyber security policy with the evolution and advancements terrorist threats).

technology defense equipment geared more for cyber warfare than artillery warfare.[3] The word 'SAFETY' is an acronym for 'Support Anti-Terrorism by Fostering Effective Technologies'.[4] Furthermore, the act awarded liability protection to defense contractors ("contractors") to manufacture defense equipment after a "certified" terrorist event happened.[5]

With increased terrorist activity, the SAFETY Act introduced a new type of equipment used for protecting American lives during a vulnerable time.[6] Additionally, limiting contractor liability encourages more contractors to develop cyber products that would prevent terrorist attacks, including cyber-attacks.[7] Moreover, after the equipment was built, it was readily available for the Department of Defense to deploy into anti-terrorism missions.[8]

The Secretary of Defense has authority to target rogue actors who launch cyber-attacks against the U.S. Government.[9] Additionally, other Federal agencies such as the National Security Agency (NSA) have authority to approve or disapprove the cyber equipment

---

[3] *See Support Anti-Terrorism by Fostering Effective Technology Act of 2002 SAFETY Act*, USCG-2003-154256 U.S.C. § 441 (2002) [*hereinafter* SAFETY Act] (illustrating the background of the safety SAFETY Act and the purpose it serves).
[4] *See id.* (explaining that the SAFETY Act "provides critical incentives for the development and deployment of anti-terrorism technology by providing liability protections for providers of 'qualified anti-terrorism technologies.'").
[5] *See id.* (highlighting that the purpose of the rule is to facilitate and promote the development and deployment of anti-terrorism technologies that will save lives); *see also Certified Act of Terrorism*, IRMI GLOSSARY OF INS. & RISK MGMT. TERMS (Apr. 14, 2017), *archived at* https://perma.cc/98G6-QANF (outlining the extensive requirements to be considered a certified act of terrorism and providing a definition of a "certified act of terrorism").
[6] *See* 153 Cong. Rec. H855-01, 2007 WL 162353 (Jan. 23, 2007) (providing a statement of Congressman Jim Langevin).
[7] *See id.* (highlighting conversation amongst congressman pertaining to the steps that the department of homeland security needs to take when monitoring anti-terrorism technology).
[8] *See* 6 U.S.C.A. § 441 (2002) (establishing where and when the equipment will be used).
[9] *See* 10 U.S.C.A. § 130g (2015) (noting existence of appropriate authorization to conduct a military cyber operation in response to "malicious cyber activity carried out against the United States or a United States person by a foreign power").

that assists military personnel on deployment.[10] Further, President Obama specifically referenced encryption equipment as a means to handle cyber threats in the National Defense Authorization Act (NDAA).[11]

One particular type of equipment with 'Tactical Local Area Network Encryption' (TACLANE) capability is the TACLANE encryptor, sold by the contractor General Dynamics, which can both ward off attacks and serve as a private highway for classified information.[12] The TACLANE encryptor is a piece of hardware embedded with computer software that protects highly sensitive data and seals classified communication.[13] Moreover, TACLANE is an essential part of the Army's WIN-T program which has its own line item in the NDAA.[14] Further, while building such equipment, contractors

[10] *See* 50 U.S.C.A. § 3617 (2004) (highlighting the National Security Agency Emerging Technologies Panel' which reports to the NSA director about technological advances in encryption).

[11] *See National Defense Authorization Act for Fiscal Year 2016*, H.R. 1735, 114th Cong. (2016) (pointing to the President's recognition of cybersecurity provisions that are necessary for an increasing threat).

[12] *See TACLANE Network Encryption*, GENERAL DYNAMICS MISSION SYSTEMS, INC. (Sep. 25, 2016), *archived at* https://perma.cc/7GJP-W2LH (illustrating that TACLANE encryptors provide high speed solutions to protect network information against cyber threats); *US Federal Business Opportunity: Other Defense Agencies: TACLANE KG175GM (x4) IG Rack Mount Shelf (x2)*, IT BRIEFING (Jan. 14, 2017), *archived at* https://perma.cc/28SM-H8QK (highlighting a government solicitation for TACLANE encryptors and the types of information within the solicitation).

[13] *See TACLANE Network Encryption*, *supra* note 12 (explaining TACLANE has high speed security solutions by offering simultaneous IP and Ethernet capabilities).

[14] *See National Defense Authorization Act for Fiscal Year 2016*, H.R.1735, 114th Cong. § 237(b)(4) (2016) (showing the WIN-T line item in the defense bill); *see also* GENERAL DYNAMICS, *The Mobile Expeditionary Soldier's Network*, WIN-T (2017) (explaining the background of the WIN-T program). WIN-T is a telecommunication system that enables soldiers to communicate with each other by using voice or visual communications. *Id.* at 5, 22. Further, it is an advanced system that also uses TACLANE encryptors to prevent adversaries from hacking into the soldier communication. *Id. See also* Sandra Jontz, *U.S. Army's Deployed WIN-T Program Software Reduces System Management Complexity*, AFCEA.ORG (Jan. 18, 2017), *archived at* https://perma.cc/8HQR-K88T (describing the type of software embedded in Win-T that's increased its functionality and overall improvement).

must comply with federal regulations that prevent them from discussing or disclosing proprietary information about encryption equipment and programs such as WIN-T.[15]

First, this Note will establish how cyber warfare has influenced contractors to build more encryption equipment in the twenty first century.[16] Second, this Note will explore how lawmakers and government agencies were prompted to implement legislation and impose regulations geared towards cyber security and terrorist threats.[17] Third, this Note will take the language from such legislation and federal acquisition regulations and explain how contractors must comply.[18] Fourth, this Note will explore how such regulations and agency demands affect the contractor while they build such equipment.[19] Finally, this Note will highlight the actual equipment used, its functionality, and the competition between contractors to build the best high technology military equipment for our military.[20]

II. History

The evolution of warfare from artillery to cyber is challenging for law makers and federal agencies to handle because cyberwar is an unfamiliar threat.[21] Further, military conflicts previously involved

---

[15] *See Federal Acquisition Regulation Site* (Oct. 21, 2016), *archived at* https://perma.cc/36F9-WJBV (showing the significance of FAR site for government contractors to reference).

[16] *See infra* Section II. (explaining the evolution of warfare from artillery to cyber).

[17] *See infra* Section II. (describing the applicability of the SAFETY ACT).

[18] *See infra* Section II. (outlining the required regulations that contractors must comply with when building government products).

[19] *See infra* Section II. (analyzing the regulation system that enforces contractor compliance).

[20] *See infra* Section III. (focusing on certain types of equipment built by different contractors).

[21] *See* Katie Bo Williams, *Senate Bill Would Require the Administration to Define 'Cyber War'*, THEHILL.COM (May 11, 2016), *archived at* https://perma.cc/RH3W-UP8D (explaining the difficulty that law makers and intelligence communities have writing laws pertaining to cyber warfare). Senators are concerned with the lack of timeliness in developing cyber legislation that defines and addresses cyber-attacks. *Id.* Given the increasing prevalence of cyber warfare, legislators have delayed developing laws pertaining to cyber-attacks because such attacks are new and unfamiliar to the country. *Id.*

physical force and imposing one's armed forces against the enemy[22], rather than imposing sophisticated technology attacks on the enemy's computer network.[23] Additionally, it is challenging for a targeted entity of a cyber-attack to identify who launched or directed the attack, if it is a cyber-attack, or whether the cyber situation is just a network malfunction.[24] Moreover, the targeted entity may be delayed in recognizing that it was a victim of cyber warfare.[25]

Despite the complexity of a cyber-attack, the SAFETY Act prompted contractors to build equipment and provide services so subjected entities could withstand attacks.[26] The role of the SAFETY Act is to "provide important legal liability protections for providers of Qualified Anti-Terrorism Technologies - whether they are products or services and encourage the development and deployment of effective anti-terrorism products and services by providing liability protections."[27] Additionally, the newly manufactured 'Anti-Terrorism Technology' has made the U.S. military even more formidable

[22] *See id.* (explaining how "[t]he bill would require policymakers to consider the ways in which the damage from a cyberattack might mirror a conventional attack — such as casualties or physical destruction").
[23] *See* HEATHER H. DINNIS, CYBER WARFARE AND THE LAWS OF WAR, 23, 75 (James Crawford & John Bell eds., 2012) (explaining war as a contention between two states for the purpose of physically overpowering each other). Dinnis goes further in explaining that diplomacy, economic incentives, political pressure, etc. played big roles in using armed forces. *Id.* at 23. Cyber-attacks don't revolve around political ramifications because it is difficult to identify who the attacker is most of the time. *Id.* at 75.
[24] *See* Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 441-43 (2011) (highlighting the difficulty in recognizing cyber-attacks and the attacking nation making it difficult to respond to the threat accordingly given the uncertainty of where the attack came from).
[25] *See id.* at 444 (explaining a delayed reaction and lasting harm a cyber-attack inflicts on an entity).
[26] *See* SAFETY Act, *supra* note 3 (providing background on what prompted the enactment of this legislation).
[27] *See id.* (highlighting the exact purpose of the SAFETY Act).

than it was before.[28] Yet, cyber warfare is the exact opposite of warfare used during the American Revolution, where the opposition lined up across from one another engaged their artillery.[29]

A cyber-attack is defined as, "the use of deliberate actions--perhaps over an extended period of time--to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks".[30] To deal with such attacks, the SAFEY Act prompted contractors to build equipment that would protect targeted networks from being harmed.[31] Yet, the SAFETY Act is a subsidiary to the 'Homeland Security Act of 2002,' which was first enacted to analyze cyber security-risk situations and the types of 'critical infrastructure' that would be attacked from cyber warriors.[32] After the Homeland Security act analyzed and identified the type of networks vulnerable

[28] *See* Dinnis, *supra* note 23, at 22 (highlighting the technological advancements in U.S. Military force). The military's adoption of high technology equipment has enhanced its ability to inflict force faster which leads to more effective missions. *Id.*
[29] *See* Dinnis, *supra* note 23, at 23 (distinguishing how traditional warfare consisted of two sides trying to overpower each other rather than the new technological purpose behind warfare); *Your Gateway to the American Revolution,* AMERICAN REVOLUTION (Oct. 23, 2016), *archived at* https://perma.cc/4NFX-E4NK (proclaiming that "[w]hen setting up forces for a battle, all the available guns would usually be arranged into a "Grand Battery" deployed in the center of the line of battle").
[30] *See* John Denver & James Denver, *Cyberwarfare: Attribution, Preemption, and National Self Defense*, 2 J.L. & CYBER WARFARE 25, 26-29 (2013) (discussing the "Effects Test" to "define when cyberattacks constitutes an armed attack that can be responded to in self-defense").
[31] *See* SAFETY Act, *supra* note 3 (explaining SAFETY Act extends "government contractor defense" to manufacturers of qualified anti-terrorism technologies, which is an affirmative defense that may immunize sellers from liability).
[32] *See* 6 U.S.C.A. § 131 (2002) (defining "critical infrastructure information" as "information not customarily in the public domain and related to the security of critical infrastructure or protected systems."); Beth Rowen, *Post-9/11 Changes by the U.S. Government*, INFOPLEASE (Jan. 12, 2017), *archived at* https://perma.cc/4R5S-TG6U (noting the Secretary of Homeland Security is tasked with "coordinating a national strategy to safeguard the country against terrorism."). The DHS implemented the National Cybersecurity Protection System to strengthen security of the country's cyber network and ward off cyberterrorist attacks. *Id.*

to attacks, the SAFETY act approved the type of technology necessary to protect such networks.[33] Thus, commencement of the manufacturing of high technology defense equipment started because of these two pieces of legislation.[34]

A popular practice exercised by vulnerable companies with big data is encryption, specifically, hardware encryption that protects company data at rest.[35] Moreover, encryption is gaining popularity because modern warfare consists of hostile computer attacks directed at an adversary's computer network with large amounts of data.[36] Therefore, military customers ("customer(s)") use a specific type of a hardware encryption device known as the TACLANE encryptor, built by the contractor, General Dynamics Mission Systems, Inc., which is hardware equipment built with an incorporated software code to encrypt data.[37] The demand for hardware encryptors has increased, and TACLANE encryptors "provide high-speed interoperable solutions to protect company networks and information against evolving cyber threats."[38] However, those who build such encryptors must comply

---

[33] *See* 6 U.S.C.A § 212(4) (describing how "Critical Infrastructure Protection Program" operates, including "communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from [the effects of cyberattack].").

[34] *See* Rowen, *supra* note 32 (delineating that after the September 11, 2011 attacks, President George W. Bush adopted strategy using sophisticated technology to combat terrorism).

[35] *See* Daniel Brecht, *Tales from the Crypt: Hardware vs. Software*, INFOSECURITY (Oct. 23, 2016), *archived at* https://perma.cc/X9WX-AT89 (justifying the use of hardware encryption to protect company's financial, healthcare, and technical data).

[36] *See* Dinnis, *supra* note 23, at 167 (explaining that control over another computer network by electronic means is a direct participation in hostilities). Encryption has become a standard practice used by military personnel because of how readily available encryptors are, and because military computer networks could be decimated by a cyber-attack if an encryptor wasn't used. *Id.*

[37] *See General Dynamics Adds New NSA-certified TACLANE-FLEX Type 1 Network Encryption Platform to Secure Product Portfolio*, GENERAL DYNAMICS (July 27, 2017), *archived at* https://perma.cc/RNX5-YYF4 (describing TACLANE-FLEX as having an "innovative design" that can evolve to meet the dynamic future needs of its customers).

[38] *See General Dynamics to Show Innovative Solutions for U.S. Marine Corps at Modern Day Marine 2017*, PR NEWSWIRE (Sept. 13, 2017), *archived at* https://perma.cc/7KQT-HLVD (noting that TACLANE is the "world's most widely deployed Type 1 encryptor"); *General Dynamics Adds New NSA-certified*

with Federal Acquisition Regulations (FAR) due to the proprietary and sometimes classified data that is used to manufacture such equipment.[39]

The FAR is a set of regulations that dictate how contractors write their contracts, build equipment, share data, impose liability, provide cost and pricing data, and bid on solicitations.[40] For example, a prime contractor, as an entity, is responsible for attaching pertinent FAR clauses in a contract with a customer, or with a sub-contractor working for the prime contractor to develop a product.[41] Further, attaching FAR clauses to contracts is an attempt to shield both parties from liability by showing that both the buyer and the seller are in compliance with the FAR.[42]

TACLANE-FLEX Type 1 Network Encryption Platform to Secure Product Portfolio, *supra* note 37 (stating is designed to meet the fluid demands of encryption demands).

[39] *See Federal Acquisition Regulation Site*, *supra* note 15 (setting forth the various FAR clauses that government contractors must comply with); *see also* FAR 15.600-15.609 (2014) (listing clauses such as 15.609 which enforce non-disclosure of proprietary information on government solicitations asking for bidders); Blake Wetterauer, *NAICS, CAGE AND OTHER GOVERNMENT CODES*, ONVIA (Feb. 2, 2016), *archived at* https://perma.cc/B37F-5K23 (highlighting the important codes and systems used as identifiers by many contractors). Prior to all government transactions, the contractor is required to provide its DUNS, NAICS, and CAGE codes to the government agency to certify that it is a reputable contractor selling a reputable product or service. *Id.*

[40] *See Federal Acquisition Regulations (FAR)*, U.S. SMALL BUSINESS ADMINISTRATION (Oct. 23, 2016), *archived at* https://perma.cc/KSX5-CD9W (explaining how the FAR is a "substantial and complex set of rules governing the federal government's purchasing process" with government contractors); *see also* Lyndon Dacuan, *Subcontract Flow-Down Clauses Explained*, ONVIA (June 3, 2010), *archived at* https://perma.cc/J4MV-TRZM (describing the differences in subcontractor FAR flow-downs and how the prime contractor contract process involves a flow down clause solely between the prime contractor and the subcontractor, but not the government customer or agency). Yet, many times a government agency buys from a prime contractor who then subcontracts the work out to another contractor, known as the 'subcontractor.' *Id.* Usually, the government agency attaches (flows down) FAR clauses to the prime, who then must attach such clauses in the contract with the subcontractor. *Id.*

[41] *See Federal Acquisition Regulations (FAR)*, *supra* note 40 (focusing on the government contracting process).

[42] *See* Dacuan, *supra* note 40 (detailing why FAR compliance is necessary to avoid costly errors and potential legal problems).

There are many types of FAR clauses that contractors need to comply with during performance of a contract.[43] But, one of many clauses used for cyber security purposes is FAR clause 52.204-21 which states that, "[t]he Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems," and then lists the necessary safeguarding procedures.[44] Additionally, the Department of Defense implemented DFAR 252.204–7012[45] which states that, "[if] the Contractor discovers a cyber-incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract the Contractor shall," and then lists the methods by which the contractor must report the cyber incidents.[46] Moreover, during performance of a contract, it is likely that proprietary information will be exchanged between a contractor and a customer.[47] Thus, clause FAR 252.227–7013 enforces ownership rights of shared proprietary data, even if disclosed to a customer solely for contract purposes.[48] Moreover, TACLANE encryptors are mainly used to protect the data referenced in FAR 252.227–7013 because such specialized data separates contractors from others, and if disclosed, will result in a contractor losing its competitive edge over another contractor.[49]

---

[43] *See Federal Acquisition Regulation Site*, *supra* note 15 (highlighting different FAR clauses that pertain to different types of items and service contracts).
[44] *See* 48 C.F.R. §52.204–21 (2016) (explaining specific FAR clause pertinent to the protection of proprietary information used in performance of the contract).
[45] *See* 48 C.F.R. § 252.204–7012 (2016) (discussing the DFAR clause 'Safeguarding Covered Defense Information and Cyber Incident Reporting').
[46] *See id.* (explaining the specific DFAR in greater detail as it pertains to cyber incident reporting); *see also* SUSAN B. CASSIDY ET AL., *Department of Defense Issues Final Rule – Network Penetration Reporting and Contracting for Cloud Services*, 3 PRATT'S GOV'T CONT. L. REP. 10, 12-9 (Meyerowitz, et al., LexisNexis & A.S. Pratt, 2017) (distinguishing between regulations and statutes for cyber incident reporting and proprietary data); *see also* 10 U.S.C. § 391 (2015) (addressing the various procedures to follow when reporting cyber incidents).
[47] *See* 10 U.S.C. § 391 (2016) (explaining the likely disclosure of proprietary information in that may warrant reporting).
[48] *See* 48 C.F.R. § 252.227–7013 (2015) (discussing how this FAR clause protects technical data from being stolen by customers or third parties).
[49] *See id.* (illustrating how data must remain inside the company in order for the company to remain competitive within the defense industry).

In addition to TACLANE, another military program used by Army customers is titled the War Fighter Information Network Tactical (WIN-T).[50] WIN-T is an Army telecommunications system that consists of satellites transported by Humvees, unmanned aerial vehicles, 'manpack' radios, ruggedized computers, tactical relay towers, and TACLANE encryptors that ultimately enable soldiers to communicate faster and more effectively with each other during contingency operations.[51] More importantly, WIN-T contains a cyber-capability that effectively encrypts soldier communication and allows personnel at command posts (connected to the network) to 'drill down' into the weeds of the network and hunt for adversaries who try to penetrate the soldier's communication.[52] Yet, with such an advanced system comes more regulations for contractors to comply with and ensure that there is no disclosure of classified technical data or software codes while building cyber systems.[53] For example, contractors that build

WIN-T comply with DFAR clause 252.239-7016 which is titled, 'Telecommunications Security Equipment, Devices, Techniques, and Services,'[54] and was written to regulate contractor telecommunication systems which are defined as:

---

[50] *See National Defense Authorization Act for Fiscal Year 2016*, *supra* note 14 (identifying the WIN-T budget allocation as one of the largest line items in 2016 defense budget).

[51] *See* General Dynamics, *supra* note 14, at 20-21 (describing WIN-T and how it operates to enable faster and more efficient communication between soldiers). One of many technological advancements, WIN-T has saved lives by allowing soldiers to communicate faster and use visuals to warn of enemy activity. *Id.*; 10 U.S.C. § 101 (2013) (providing the definition of a "contingency operation."). A contingency operation "is designated by the Secretary of Defense as an operation in which members of the armed forces are or may become involved in military actions, operations, or hostilities against an enemy of the United States or against an opposing military force". *Id.*

[52] *See* General Dynamics, *supra* note 14, at 22 (noting "[a]t every node, WIN-T incorporates cyber protections to keep communications secure").

[53] *See Federal Acquisition Regulation Site*, *supra* note 15 (defining "Federal Acquisition Regulation (FAR) as a substantial and complex set of rules governing the federal government's purchasing process."). "Its purpose is to ensure purchasing procedures are standard and consistent, and conducted in a fair and impartial manner." *Id.*

[54] *See* 48 C.F.R. § 252.239–7016 (2015) (providing a specific FAR regulation that pertains to the construction of "telecommunication systems," such as WIN-T).

> voice, record, and data communications, including management information systems and local data networks that connect to external transmission media, when employed by Government agencies, contractors, and subcontractors to transmit (i) Classified or sensitive information; (ii) Matters involving intelligence activities, cryptologic activities related to national security, the command and control of military forces, or equipment that is an integral part of a weapon or weapons system; or (iii) Matters critical to the direct fulfillment of military or intelligence missions.[55]

Overall, WIN-T is an example of the advanced technological systems used by the military to ready military personnel for their transition into a world of cyber warfare.[56]

Despite the regulations that protect the disclosure of proprietary data, there are still cases and stories of contractor employees violating FAR regulations that are being prosecuted for those violation.[57] For example, a Booze Allen Hamilton employee was recently arrested for stealing classified information which likely violated FAR 252.227–7013.[58] Moreover, bribery cases exist where contractors provided customers with discounts and kickbacks for choosing to do business with them after completion of a competitive bidding process.[59]

---

[55] *See id.* (highlighting the language of a specific FAR clause).
[56] *See The Mobile, Expeditionary Soldier's Network*, WIN-T (2016) (attesting to the overall effectiveness of WIN-T and its ability to assist the military in an age of cyber warfare).
[57] *See* Matt Zapotosky et al., *NSA Contractor Charged with Stealing Top Secret Data*, WASH. POST (Oct. 5, 2016), *archived at* https://perma.cc/PG5T-NJ7E (illustrating how government contractor employees sometimes do not comply with the FAR and are capable of stealing top secret data from their employer).
[58] *See id.* (explaining the specific FAR clause a rogue employee violated); *see also* 48 C.F.R. § 252.227–7013 (2015) (emphasizing what constitutes the unauthorized disclosure of "technical data outside the Government").
[59] *See Former Army Official and Contractor Indicted for Bribery Scheme Involving Contracts at Aberdeen Proving Ground*, UNITED STATES DEPT. OF JUSTICE (Jul. 13,

In addition to cases of noncompliance and illegality, contractors also bring allegations against each other through a legal process known as 'bid protests,' where they challenge each other's awarded contracts through the Government Accountability Office.[60] Bid protests involve one contractor alleging that the awardee (winning contractor) fraudulently misrepresented information on their proposals in an effort to entice the customer into buying from them rather than other contractors.[61] Thus, competition for a customer's business prompts contractors to take both legal and illegal action against each other just to be awarded a contract[62]. Moreover, cyber encryption equipment is a popular product line that all contractors are currently competing to make in hopes of winning their next contract with a military or civilian customer.[63]

Although FAR clauses, bid protests, and provisions of SAFETY Act legislation are important, International Humanitarian Law (IHL) laid the foundation for the aforementioned subjects to

---

2016), *archived at* https://perma.cc/K74H-GZKH (providing an example of one instance where a government contractor bribed their customers to award them contracts due to the competitive nature of the industry).

[60] *See* Matter of ManTech Advanced Systems International, Inc., 1994 WL 242282, at *1 (Comp. Gen. May 11, 1994) (illustrating an example of a "bid protest" for a lost contract); Matter of ManTech Field Engineering Corporation, 1992 WL 70971, at *1 (Comp. Gen. Mar 27, 1992) (portraying a bid protest against a contractor for misrepresenting the amount of capable and readied employees on the proposal). ManTech protested that the awardee misrepresented how many ready personnel were available to work on the first day just to be awarded the contract. *Id. See also* U.S. Government Accountability Office, *Bid Protests*, GAO.GOV (Jan. 21, 2017), *archived at* https://perma.cc/WQS5-7D5E (describing GAO as providing an "objective, independent, and impartial forum" for resolving disputes between prospective government contractors.).

[61] *See* U.S. GOVERNMENT ACCOUNTABILITY OFFICE, BID PROTESTS AT GAO: A DESCRIPTIVE GUIDE 8 (2009) (explaining protests generally filed alleging "defective solicitations" and other procurement actions).

[62] *See* ManTech Field Engineering Corporation, 1992 WL 70971, at *1 (Comp. Gen. Mar 27, 1992) (vindicating ManTech Field Engineering's claim alleging Systems Engineering & Management Associates, Inc. misrepresented the availability of its personnel in obtaining government contract).

[63] *See* Matter of: ManTech Advanced Systems International, Inc., 1994 WL 242282, at *1 (Comp. Gen. May 11, 1994) (opining that there are more government contracts available for cyber and electronic programs, such as those that require "engineering services to support the Army's TROJAN electronic communications and reconnaissance system").

stand on.[64] Moreover, the 1949 Geneva Convention implemented such humanitarian laws to prevent armed conflict between state actors.[65] However, it is difficult to apply International Humanitarian Laws to terrorist cyber activity because IHL was originally created to pre-empt armed warfare amongst known actors rather than cyber warfare amongst undisclosed terrorists.[66] Therefore, the complexity of a computer network attack can no longer be dismissed as a rare occurrence, but rather must be accepted as an evolving form of warfare that needs to be prepared for by United States Intelligence Agencies.[67] Further, contractors sell their products internationally to 'foreign actors,' and their specifications, drawings and other documents provided during the proposal process may contain technical data whose export may be restricted by the ARMS Export Control Act or

[64] *See* Kenneth Watkin, *Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict*, 98 AM. J. INT'L L. 1, 2 (2004) (positing that the International Humanitarian Law framework challenges traditional ideas about the use of force in armed conflict, including cyber-attacks).

[65] *See* International Committee of the Red Cross, *The Rule of Law at the National and International Levels: ICRC Statement to the United Nations, 2016*, ICRC (Oct. 7 2016), *archived at* https://perma.cc/3JEC-9NCR (connecting IHL and the Geneva Convention through their common foundation in the "rule of law"); Dinnis, *supra* note 23, at 233 (explaining the prohibiting language of International Humanitarian Law regarding the digital environment); Christopher Sawin, *Creating Super Soldiers for Warfare: A Look into The Laws of War*, 17 J. HIGH TECH. L. 105, 113 (2016) (stating that the purpose of the Geneva Convention was originally created to protect civilians from warfare).

[66] *See* Watkin, *supra* note 64, at 9 (discussing the "complexity" of international humanitarian laws and whether such laws apply to terrorist contemporary conflict).

[67] *See* Dinnis, *supra* note 23, at 239 (illustrating how the U.S. government originally dismissed the idea of attacks through computer networks and later understood the significance of such attacks). The U.S. was not prepared for cyber-attacks, but began preparing and training for them after collecting evidence from reoccurring terrorist cyber activity. *Id.*

Executive Order 12470.[68] Additionally, a violation of these export laws are subject to severe criminal penalties.[69]

III. Facts

The September 11, 2001 terrorist attacks sparked an increase in terrorist activity and prompted the U.S. government to build cyber equipment that would both deter and locate terrorist activity.[70] However, despite existing humanitarian laws for armed conflicts between state actors, the U.S. government still underestimated the opposition and the amount of planning that went into a cyber-attack.[71] For instance, in 2002, while on patrol in Afghanistan, U.S. troops found an Al Qaeda laptop which indicated a strong interest in computer network attacks.[72] Further, another Al Qaeda laptop was seized in Ka-

[68] *See* 22 U.S.C.A §2751 (2016) (explaining the need for international defense cooperation and military export controls); Exec. Order No. 12470, *Continuation of Export Control Regulations* (Mar. 30, 1984) (illustrating that "unrestricted access of foreign parties to United States commercial goods, technology, and technical data" posed an "extraordinary threat to the national security, foreign policy and economy of the United States"). It is important for contractors to comply with export control laws for national security. *Id.* Further, it is important that a foreign actor does not mistakenly receive unauthorized proprietary data for fear they may use or sell to a rogue actor. *Id.*

[69] *See ITAR Compliance Requirements*, SKYHIGH (Apr. 24, 2017), *archived at* https://perma.cc/FFW7-GTLS (stating that "criminal penalties can include 10 years imprisonment and fines of up to $1 million per violation").

[70] *See* Rowen, *supra* note 32 (describing how 9/11 prompted the creation of the Department of Homeland Security as well as legislation to combat cyberterrorism). Coupled with the creation of agencies and laws, the National Cybersecurity Protection System was created because of the increasing prevalence of cyber warfare. *Id.*

[71] *See* Dinnis, *supra* note 23, at 241 (describing that under the term "installations containing dangerous forces," the terrorist threats were under estimated); *see also* Watkin, *supra* note 64, at 3 (discussing the complexity of Al Qaeda activity after the September 11 terrorist attacks).

[72] *See* Dinnis, *supra* note 23, at 239 (illustrating a specific example of Al Qaeda activity that showed their interest in computer network attacks). After searching the laptop, "computer forensics showed that the laptop had multiple visits" to sites with sabotage, software, and 'cracking' information. *Id.*

bul, Afghanistan that had architectural models of a dam as well as engineering software that enabled the dam to operate.[73] Moreover, it is possible that future terrorist attacks will target large computer networks in banks, military bases, power plants, air traffic control centers, and water systems because civilians depend heavily on each of these targets and cyber terrorists could be aware that such a malfunction within the network of each target would "produce a spectacle of shocking consequences." [74]

In addition to large-entity computer networks, complex military weapon systems are also at risk of being hacked, especially in a nuclear proliferation climate.[75] For instance, the defense contractor, Raytheon, builds an air and missile defense system that must be protected at all times from cyberterrorism so that U.S. air and missile defense capability can be properly maintained.[76] There is also an unmanned underwater vehicle known as the 'knifefish,' built by General Dynamics, which is deployed by combat ships to detect underwater mines that, if undetected, would cause significant damage to combat ships.[77] Therefore, the software in the knifefish is also pro-

---

[73] *See* Dinnis, *supra* note 23, at 240 (providing another example of when an Al Qaeda laptop was found to have engineering software codes and architectural models of a dam to potentially issue a cyber-attack against the computer network and prevent the dam from operating).

[74] *See* Sue Marquette Poremba, *Cyber Terrorist Threats Loom 10 Years After 9/11*, NBCNEWS.COM (Sep. 9, 2011), *archived at* https://perma.cc/RUB4-7QUK (illustrating how large entity computer networks heavily depended on by civilian populations could be targeted by cyber terrorism); Watkin, *supra* note 64, at 14 (emphasizing the large scale and effects of contemporary cyberterrorism and the response effort that will be needed).

[75] *See* Watkin, *supra* note 64, at 14 (rationalizing why a cyber terrorist would be incentivized to operate outside the traditional scope of weapons of mass destruction).

[76] *See* Abraham D. Sofaer, *On the Necessity of Pre-Emption*, 14 EUR. J. INT'L L. 209, 210-11 (2003) (outlining various justifications behind pre-emptive actions against potential terrorist threats); *Global Patriot Solutions*, RAYTHEON (Nov. 22, 2016), *archived at* https://perma.cc/P2PE-QFC7 (introducing Global Patriot Solutions: a ballistic missile system that could be targeted by cyber-attacks).

[77] *See Knifefish Unmanned Undersea Vehicle*, GENERAL DYNAMICS (Nov. 22, 2016), *archived at* https://perma.cc/MAV8-BTN8 (promoting the knifefish, an undersea vehicle which detects mines for military vessels); Megan Eckstein, *Navy's First Operational MQ-4C Triton Squadron Stands Up This Week*, USNI NEWS (Oct. 25, 2016), *archived at* https://perma.cc/R4UW-VD9R (highlighting the Triton

prietary information that must not be disclosed to cyber terrorist actors.[78] With that, the software built into complex military weapons and equipment must be secured so that they can function and protect "key locations" and "critical infrastructure[e] within the U.S.[79]

As a result of an increased demand for cyber products, contractors have changed their company strategy to build more cyber products and meet the needs of the customer.[80] Additionally, contractors spend 'research and development' money on new cyber products because of the international climate of increased cyber threats from countries like North Korea and China.[81] Moreover, Russia's suspected attack on Ukraine's power grid increased the world's paranoia regarding cyber-attacks and thus elevated countries' development of cyber equipment.[82] Furthermore, global expenditures for

program, which involves an unmanned aerial vehicle equipped with sensors to send encrypted signals to personnel on the ground).

[78] *See General Dynamics Completes Comprehensive Risk Reduction Program for Knifefish UUV Program*, GENERAL DYNAMICS (Aug. 6, 2013), *archived at* https://perma.cc/YUY9-FTH6 (discussing the development of the software system for the knifefish).

[79] *See* Sofaer, *supra* note 76, at 210 (describing how technologically sophisticated systems are used to protect the U.S. from cyber-attacks and prevent vulnerabilities).

[80] *See* John Persinos, *These 3 Aerospace Stocks Offer a Sharper Bite Than the FANG Group*, THESTREET.COM (Oct. 11, 2016), *archived at* https://perma.cc/RYA5-JFM4 (demonstrating how defense contractors such as Raytheon are diversifying into cybersecurity and spending internal money on developing cyber products). In order for defense contractors to survive as a company and generate revenue they need to change the products they sell. *Id.* As a result, defense contractors are spending large sums of money developing new cyber products because that is what the military customer wants to buy in the future. *Id.*

[81] *See* Doug Crowder and David Radi, *Now Hear This - It's Time for a Cyber Moon Shot*, U.S. NAVAL INSTITUTE (Oct. 2016), *archived at* https://perma.cc/9FTS-45H4 (disclosing the many instances of cyber-attacks from foreign governments like North Korea's attack on SONY and the suspected Chinese attack on both defense contractors and the U.S. Office of Personnel Management). Increased cyber-attacks have created panic amongst military customers which has made them demand more cyber products from defense contractors. *Id.*; David S. Gallacher, *The Times they are a Changin' – Independent Research and Development May Not Be So "Independent" Any More*, GOVERNMENT CONTRACTS & INVESTIGATIONS BLOG (Apr. 18, 2011), *archived at* https://perma.cc/WC29-GHTR (describing relevant background information regarding research and development in government contracting).

[82] *See* Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016), *archived at* https://perma.cc/5SD3-5J3Q (explaining

cyber products and services in 2016 have totaled at $73.6 billion with the U.S. having the largest cyber security market in the world at $31.5 billion.[83] Additionally, customers are awarding more business to contractors for cyber products so they can compete with other customers and prevent their computer networks from being hacked.[84]

Although the DoD aims to reduce its spending, major contractors such as Lockheed Martin, General Dynamics, Raytheon, Boeing, and other smaller contractors have all increased their revenue from winning multimillion dollar contracts to develop new cyber equipment.[85] Additionally, in accordance with President Barack Obama's

---

the suspected Russian hacker's strategy in attacking power centers in Ukraine); Robert Windrem, *Timeline: Ten Years of Russian Cyber Attacks on Other Nations*, NBC NEWS (Dec. 18, 2016), *archived at* https://perma.cc/F7QB-FHE9 (drawing attention to the more than a dozen significant cyber-attacks launched by Russia against foreign countries in the past decade). Russia has created world-wide news about their cyber-attacks on other countries. *Id.* Specifically, Russia's cyber-attacks are motivated by politics in hopes of thwarting their victim country's elections. *Id.*

[83] *See* Sean Michael Kerner, *Global Cyber-Security Spending to Top $100B by 2020: IDC*, EWEEK (Oct. 13, 2016), *archived at* https://perma.cc/6W68-29YP (highlighting the global increase in demand for cyber security products and services). No company wants to be the next victim of a cyber-attack and therefore spends large sums of money on cyber equipment to protect their company's brand. *Id. See also* 6 U.S.C. §395 (2004) (describing how the U.S. is prevented from trading with a foreign entity categorized as an inverted domestic corporation). While contractors partake in global expenditures with other countries, they must first figure out if the foreign entity they do business with is an "inverted domestic corporation." *Id.*

[84] *See* Zacks Equity Research, *Defense Stock Roundup: Honeywell Cuts Q3 View; Big Wins at BAE Systems, General Dynamics*, ZACKS (Oct. 12, 2016), *archived at* https://perma.cc/33CR-RND2 (illustrating the lucrative contracts awarded to Lockheed Martin from the U.S. Navy worth $215 million). Lockheed is a major defense contractor that wins hundreds of millions of dollars' worth of contracts from the Navy for services on electronic warfare portfolios. *Id. See also* Deloitte Insights, *2016 Global Aerospace and Defense Sector Poised to Resume Growth*, DELOITTE (Jan. 2016), *archived at* https://perma.cc/HP7M-8ZDQ (explaining how defense budgets are increasing and revenue within the defense industry is growing because of heightened security risks around the world).

[85] *See* Mark Karlin, *Private Defense Contractors Need War to Keep Profits High*, BUZZFLASH (July 17, 2015), *archived at* https://perma.cc/8VPB-ZEQJ (illustrating how most defense contractors still profited even after defense budget cuts because of the increased demand from the Iraq and Afghanistan wars); Lauren Budik, *Engility Wins $31M Contract to Provide Cybersecurity Support to DTIC*,

'small business initiative,' there is a mandated portion of the defense budget that must be spent on small-sized contractors.[86] On the other hand, the initiative also has negatively affected the defense industry because mid-size and large contractors are losing business since small companies must now be awarded contracts.[87] Further, in an attempt to win business, larger contractors misrepresent themselves as small businesses just to be awarded contracts, but suffer punishment if their tactics are discovered.[88] Yet, President Donald Trump intends to reduce government spending on defense contracts regardless of the small business initiative because contract prices are too high.[89]

WASHINGTONEXEC (Jan. 10, 2017), *archived at* https://perma.cc/C93P-9HNT (highlighting one of the many contracts recently awarded to build cyber equipment in 2017).

[86] *See Supporting Small Businesses*, WHITEHOUSE (Jan. 12, 2017), *archived* at https://perma.cc/Y4FV-TTVY (highlighting the presidential plan to assist small business contractors). Now, a majority of military customers express in their "requests for proposal" that their contracts require them to award a portion of their budget to small business contractor in addition to a larger contractor such as Lockheed Martin or Raytheon. *Id.*

[87] *See* Philip G. Bail Jr, *The Demise of The Federal Government Small Business Program*, DEFENSE ACQUISITION U. (2010) (describing how the small business initiative is also harmful to larger contractors because of the accommodations they must make for smaller contractors). Larger and mid-size companies lose contracts because of a law that sets aside federal money to be spent on smaller companies. *Id*. Thus, the initiative effects the competition, but possibly creates a balanced scale in defense contracting. *Id.*

[88] *See* 15 USC §645(d) (2013) (setting forth the various repercussions for companies who misrepresent themselves as small business contractors).

[89] *See* Zacks Equity Research, *4 Defense Stocks to Buy on the Dip After Trump's Comments*, ZACKS (Dec. 13, 2016), *archived at* https://perma.cc/CJ9P-ZTS7 (explaining how government contracts are too costly and that prices must be reduced). Originally, the stock market soared after Trump became president, but his recent public statements about overpriced defense contracts created uncertainty in the defense industry. *Id. But see* Holly LaFon, *Baron Funds Comments on Mercury Systems*, GURUFOCUS (Jan. 20, 2017), *archived at* https://perma.cc/26VN-SYFL (providing an alternative view of how a republican administration will seek to increase defense spending because there is a higher demand of complex electronic subsystems that contractors need to build their products); Michael O'Hanlon, *The Importance of Defense Spending to the Economy*, NEWSWEEK (Aug. 25, 2015), *archived at* https://perma.cc/ATL3-38TM (illustrating the benefits to consistent spending in the defense industry); Ana Radelat, *DoD, Lockheed Martin Agreement Cuts Price of F-35*, THE CT MIRROR (Feb. 3, 2017), *archived at* https://perma.cc/C39F-AVNP (analyzing how President Trump's pressure on the

Ultimately, large military expenditures are elements of the Military Industrial Complex, first mentioned by President Dwight D. Eisenhower in his Farewell Address, and enable many transactions of high-priced defense contracts.[90] President Eisenhower described the defense industry as a "permanent armaments industry of vast proportions," and is responsible for half of the federal budget.[91] Unfortunately, wars benefit the economy because they provide jobs to contractor personnel, but wartime is not an excuse for contract costs to

---

Pentagon prompted personnel within the DoD to significantly reduce the contract price of certain fighter jets); Keila Torres Ocasio, *Sikorsky Deal Cuts Pay for Future Workers*, CTPOST (Oct. 1, 2016), *archived at* https://perma.cc/7GHL-B3CS (examining how contractor personnel are now taking pay cuts as a result of a new presidential administration that will reduce DoD spending).

[90] *See* Dwight D. Eisenhower, President of the United States, Farewell Presidential Address (Jan. 17, 1961) (warning about an enlarged industry called the "military industrial complex"). President Eisenhower explained how the need for military readiness must not lead to an industry that spends too much government money and involves politics. *Id. See also* 22 U.S.C. § 2751 (1978) (introducing the Arms Export Control Act, which aims to discourage countries from participating in arms races with each other).

> Because of the growing cost and complexity of defense equipment, it is increasingly difficult and uneconomic for any country, particularly a developing country, to fill all of its legitimate defense requirements from its own design and production base. The need for international defense cooperation among the United States and those friendly countries to which it is allied by mutual defense treaties is especially important, since the effectiveness of their armed forces to act in concert to deter or defeat aggression is directly related to the operational compatibility of their defense equipment.

Id.

[91] *See* Eisenhower, *supra* note 90 (focusing on the federal expenditures for defense equipment); *What is the Military-Industrial Complex?*, MILITARY-INDUSTRIAL COMPLEX (Jan. 16, 2016), *archived at* https://perma.cc/T4DM-4SJ5 (describing the relationship between the DoD and defense contractors when making defense acquisitions); 41 U.S.C. § 3903 (2011) (explaining how the government analyzes whether a contract extension after one year is necessary, or whether the contract needs to be canceled or terminated). This statute has both a termination and cancellation clause in the event that there is not enough appropriated funds to pay for a contract performance. *Id.* Thus, this statute imposes a necessary cap on the duration of contracts if there are not any more appropriated funds to pay for the contract. *Id.*

spiral out of control just because of a high demand for cyber products to handle military conflicts.[92]

As previously mentioned, the Department of Defense (DoD) introduced a new regulation for 'cyber incident reporting' because of the significant increase across the defense industry for cyber products built with proprietary technical data.[93] The DoD also introduced this regulation for extra cautionary purposes because certain computer systems previously used by the military are now used by civilians, such as GPS systems, and any interference or disruption from a cyber-attack on such a system could significantly harm civilians.[94] Yet, to prevent cyber incident reporting from even happening, contractors usually sign non-disclosure agreements and memorandums of agreement so both parties understand that proprietary information

[92] *See* Zacks Equity Research, *supra* note 89 (explaining how Trump intends to reduce defense contract prices because they are too high). *But see* Jacob Pramuk, *Trump's First Budget Proposal Will Call For $54 Billion Increase in Defense Spending*, CNBC.COM (Feb. 27, 2017), *archived at* https://perma.cc/8Y5X-FY3F (reporting on President Trump's plan to increase the DoD budget but decrease other federal agency budgets). To illustrate the comparison between the DoD budget and other agencies: the current DoD budget is around six hundred billion dollars while the State Department's overall budget is fifty billion dollars. *Id.* Critics question why an agency with more than half of the federal budget needs to be increased. *Id.* Although Trump cut the prices of some military programs, he still plans to make the United States Military the priority in his newly expected budget. *Id.*

[93] *See* 48 C.F.R. § 252.204–7012 (2016) (referring to DFARS clause "cyber incident reporting" as it applies to technical information); Gibson, Dunn & Crutcher LLP, *New Cybersecurity Requirements for Defense Contractors Take Effect*, GIBSON DUNN (Oct. 31, 2016), *archived at* https://perma.cc/4A3N-XF8P (alerting defense contractors that "cyber incident reporting" regulations will be imposed with the newly increased demand for cybersecurity products and services). *But see* Daniel Wilson, *DOD Cyber Rule May Create as Many Problems as It Solves*, LAW360.COM (Oct. 20, 2016), *archived at* https://perma.cc/NS3T-LWQN (addressing concern that the new "cyber incident report" regulations may place extra burdens on defense contractors).

[94] *See* Dinnis, *supra* note 23, at 194 (describing how cyber incident reporting regulations are necessary more than ever because military computer technology, such as a GPS systems, are now used by civilians and preemptive measures are necessary to prevent cyber-attacks from harming civilian while they use such technology).

should not be shared with unauthorized individuals.[95] Overall, an enlarged cyber market has been good for contractors because customers are buying more cyber products and awarding larger contracts.[96]

IV. Analysis

The aforementioned sections provided context on the dynamic between contractors in an enlarging cyber market and DoD expenditures in that market. [97] The following sections will analyze whether DoD expenditures in cyber are too costly, and whether FAR regulations are enforcing accountability on contractors when performing their scope of work.[98] This Note will conclude that there may be costly defense contracts which fuel the military industrial complex, but those expenditures are necessary for the research, development,

---

[95] *See* OFFICE OF THE STAFF JUDGE ADVOCATE, ACQUIRING AND ENFORCING THE GOVERNMENT'S RIGHTS IN TECHNICAL DATA AND COMPUTER SOFTWARE UNDER DEPARTMENT OF DEFENSE CONTRACTS: A PRACTICAL HANDBOOK FOR ACQUISITION PROFESSIONALS (8th ed. 2017) (illustrating that compliance with DFARS clause 227.7103-7 'Use and Non-Disclosure Agreement' is necessary when providing a third-party computer software or other technical data).

[96] *See* Karlin, *supra* note 85 (explaining how the military industrial complex enables defense contractors to profit because customers will still award large contracts regardless of sequestration). The military industrial complex is a permanent defense industry fueled by war, so regardless of budget cuts, the federal government will still spend large amounts of money on defense equipment to ensure military readiness. *Id.*

[97] *See* Karlin, *supra* note 85 (describing how contractor employees cost more to bill than civilian employees because of the military products they work on).

[98] *See* 10 U.S.C. § 391, *supra* note 47 (displaying the steps for contractor personnel to take when reporting cyber incidents).

> Each such report shall include the following: (A) An assessment by the contractor of the effect of the cyber incident on the ability of the contractor to meet the contractual requirements of the Department. (B) The technique or method used in such cyber incident. (C) A sample of any malicious software, if discovered and isolated by the contractor, involved in such cyber incident. (D) A summary of information compromised by such cyber incident.

Id.

and use of new cyber programs requested by the U.S. military to succeed in a cyber world.[99]

Although high-priced military expenditures for cyber equipment are necessary, the spending must be controlled.[100] However, the DoD is entitled to temporarily award high-priced contracts to complete the research and development ("R&D") phase necessary to build new equipment that is ready to handle an evolving threat of cyber warfare.[101] After completion of the R&D phase, the equipment will be categorized as a steady product, but the costs to acquire such equipment must be stabilized.[102] Still, the FAR clauses must still be scaled down in R&D contracts in order to enforce accountability and structure onto the contractor who performs the work.[103]

Every FAR clause that is scaled down to a contractor from the government customer is essential to performing the contract [104] because there are clauses specifically written for cyber contracts that

---

[99] *See* Eisenhower, *supra* note 90 (addressing President Eisenhower's recognition of technological advancements in warfare). This "research has become central; it also becomes more formalized, complex, and costly. A steadily increasing share is conducted for, by, or at the direction of, the Federal government." *Id.*

[100] *See* Zacks Equity Research, *supra* note 84 (describing that certain defense contracts are too expensive, yet
mentioning certain contractors to invest in). Some of the contractors to invest in include Kratos Defense & Security Solutions, Inc., because of the innovative cyber equipment they build. *Id.*

[101] *See* Gallacher, *supra* note 81 (focusing on government spending for a contractor to research and develop new technological equipment). Innovative thinking leads to the research and development of new products, but money must first be spent on researching and developing the new product before it can enter the market to be sold. *Id.* After R&D is complete a contractor can figure out how to deal with ownership rights and disclosure or non-disclosure of proprietary information. *Id.*

[102] *See* Zacks Equity Research, *supra* note 89 (addressing how paranoia from high prices in the defense industry fades overtime). This is because "defense is essentially a non-cyclical sector, which enabled it to remain mostly stable over the years. So, it is probably safe to assume that the ongoing turmoil in the sector is going to be short lived." *Id. See also* Gallacher, *supra* note 81 (explaining the process behind internal research and development of a new product).

[103] *See* Dacuan, *supra* note 40 (describing the procedure of FAR flowdowns and how they force a contractor to comply, usually with "blanket flow-downs").

[104] *See* Dacuan, *supra* note 40 (emphasizing FAR flowdowns as a necessary and required procedure of government contracting).

must be complied with.[105] More importantly, contractors must comply with the North American Industry Classification System (NAICS), and provide a unique Dun & Bradstreet's nine-digit DUNS code and Commercial and Government Entity, or CAGE, code to show that the contractor is a reputable and accountable entity participating in a government transaction.[106] Furthermore, the product or service that is the subject of the transaction must meet the expectation of the customer[107] because the customer expects a highly technological piece of equipment with sophisticated software to compete in a cyber world.[108] Therefore, customers solicit contractors to participate in R&D contracts to build the newest software that can be embedded in encryption devices, such as the TACLANE encryptor.[109]

Additionally, R&D contracts cost the government a lot of money, however, these contracts are necessary for finding the newest

[105] *See* 48 C.F.R. §52.204–21(b) (2016) (setting forth the requirements and procedures that are safeguard Covered Contractor Information Systems); 48 C.F.R. § 252.204–7012(b)(1) (2016) (listing the cyber incident reporting requirements).
[106] *See* Wetterauer, *supra* note 39 (describing how important it is for contractors to have NAICS, DUNS, and CAGE codes to show customers that they are certified entities supplying products and services). A CAGE code is similar to the social security system in that it is a five-character ID number that identifies the contractor. *Id.* Buying customers ask contractors to provide their codes, and if a contractor does not have any of these certifications then it is a red flag to the buyer. *Id.*
[107] *See US Federal Business Opportunity: Other Defense Agencies: TACLANE KG175GM (x4) IG Rack Mount Shelf (x2)*, *supra* note 12 (displaying a military customer solicitation to show the customer's specific requirements and expectations of a contractor when supplying a TACLANE encryptor).
[108] *See* Brecht, *supra* note 35 (illustrating the security features of encryption software and how this type of software is more prevalent than hardware solutions today). "Software-based encryption often includes additional security features that compliment encryption, which cannot come directly from the hardware." *Id.*
[109] *See* Gallacher, *supra* note 81 (noting that companies are allowed to engage in R&D with the Government independent of its contracts or customers); *TACLANE Network Encryption*, *supra* note 12 (introducing the TACLANE encryptor and its software functionalities). TACLANE contains advanced encryption-based software that is responsible for its high standard of efficiency. *Id. See also* LaFon, *supra* note 89 (describing the "embedded protection capabilities" added to already-existing military hardware cybersecurity products). The added capabilities lead to an increase in purchases for Mercury's complex electronic subsystems because contractors increased their demand for such a product based on the popularized cyber market. *Id.*

and most advanced encryption methods.[110] Following completion of R&D, the developed product will improve an already existing governmental program, such as WIN-T, and increase the program's functionality and efficiency because of the advanced encryption-based software that was added.[111] Moreover, missile defense programs and underwater 'knifefish' programs have also improved from the added software that gives such programs more advanced capabilities. [112] Yet, with improved programs comes increased contract costs, potentially fueling the military industrial complex.[113] Furthermore, the increased costs in R&D influenced the implementation of DFAR rules to control R&D spending because R&D is increasing in the defense industry, but may not always be worth the expenditures.[114]

---

[110] *See* Gallacher, *supra* note 81 (discussing a proposed regulation requiring research and development contractors to report annual projects exceeding $50,000 in an effort to control costs).

[111] *See* Jontz, *supra* note 14 (highlighting the PacStar's IQ-Core Software which is ten times faster than comparable communication equipment).

> The results showed that using the software greatly improved participants' ability to successfully complete the tasks, and reduced both the time spent on the projects and the errors committed, regardless of the end user's level of computer and networking expertise. 'Participants also reported significantly higher confidence in their ability to do other, similar tasks on the equipment when using IQ-Core Software,' the study states.

Id.

[112] *See Global Patriot Solutions*, *supra* note 76 (explaining Global Patriot Solutions as an advanced missile defense program with the latest innovation in technology and manufacturing); *Knifefish Unmanned Undersea Vehicle*, *supra* note 77 (showing an advanced underwater radar detection program with enhanced mine-hunting capability).

[113] *See* Zacks Equity Research, *supra* note 89 (explaining how defense contracts are becoming too costly for the government); Eisenhower, *supra* note 90 (discussing how the defense industry has grown into a military industrial complex fueled by large defense transactions). *But see* 22 U.S.C. § 2751 (establishing that the arms export control statute regulates the amount of defense equipment manufactured and sold in an attempt to control an already massive industry from becoming overbearing in global trades).

[114] *See* Gallacher, *supra* note 81 (illustrating new, proposed DFAR rules to regulate spending on R&D contracts that costs more than $50,000.00). The government could hold contractors accountable for their R&D contracts by making the contractors provide a report on the R&D results. *Id.* Spending over $50,000.00 on R&D efforts

Although critics claim that defense programs have become too costly, the programs are fundamentally sound and essential to protecting our National Security.[115] For example, the TACLANE encryptor must first be approved by the NSA to ensure compliance with government regulations, and is then sold to credible customers.[116] Further, the WIN-T program, patriot program, and knifefish program are essential in assisting the United States execute effective missions to protect the American people because such programs can either operate in the air, land, or sea.[117] Moreover, the defense industry is a

---

alone is too much, and the government wants to see if such expenditures are worth it. *Id.* Therefore, rules are enforced to prevent R&D expenditures from getting out of hand. *Id.*

[115] *See SAFETY Act*, *supra* note 3, at 33148 (introducing the SAFETY Act and its purpose of creating anti-terrorism technology that prevents attacks and protects citizens). The implementation of this legislation raised awareness for the importance of software development and other intellectual property needed for high functioning technological equipment. *Id.*

> The SAFETY Act applies to a broad range of technologies, including products, services, and software, or combinations thereof, as long as the Secretary, as an exercise of discretion and judgment, determines that a technology merits Designation. The Secretary may designate a system containing many component technologies (including products and services) or may designate specific component technologies individually. Further, as the statutory criteria suggest, a Qualified Anti-Terrorism Technology need not be newly developed—it may have already been employed (e.g. "prior United States government use") or may be a new application of an existing technology.

Id. at 33149. *But see* DEP'T OF DEF., PRESS OPERATIONS, DOD RELEASES FISCAL YEAR 2018 BUDGET PROPOSAL REL. NO. NR-192-17 (May 23, 2017) (justifying a higher defense budget as a necessity in an increasingly dangerous world).

[116] *See* 50 U.S.C.A § 3617 (describing the National Security Agency panel which, in part, analyzes encryption equipment and its qualifications). Further, the NSA panel advises the director on R&D for cyber equipment. *Id. See also TACLANE Network Encryption*, *supra* note 12 (asserting that this type of encryption equipment, including the TACLANE encryptor, go through an NSA certification process).

[117] *See Win-T: The Mobile, Expeditionary Soldier's Network 2017*, *supra* note 14 (describing the Win-T program's effectiveness); Jontz, *supra* note 14 (explaining the new software embedded in the Win-T program and how it has made the program more effective and functional); *Global Patriot Solutions*, *supra* note 76 (explaining a popular missile defense program used by the U.S.). The missile defense program

heavily regulated industry that holds contractors accountable for excess spending and contract extensions.[118] Therefore, contracts cost the government a lot of money, but the transactions are conducted in an appropriate and necessary manner with heavy regulation, a heavy vetting process, and with strong attention to detail.[119]

Not only is the defense industry heavily regulated, but the defense industry also makes sure to award contracts to smaller defense companies so they can also compete within the industry.[120] Further, the bid-protesting process is a fair and legal process that adds accountability to the industry by allowing losing contractors to fight for business even after losing the bid to another contractor. [121] This pro-

is a necessary program to deter countries with nuclear arsenals. *Id. See also* Sofaer, *supra* note 76, at 209 (explaining how nuclear proliferation amongst countries is a global threat and needs to be pre-empted); *Knifefish Unmanned Undersea Vehicle*, *supra* note 77 (illustrating how the Knifefish's underwater capabilities detect mines and help to prevent ships from sailing into hazardous waters).

[118] *See* 41 U.S.C. § 3903 (stating the government analyzes whether a contract extension is necessary based on the amount of appropriated funding remains rule that controls R&D spending when annual costs exceed a designated dollar threshold); *see also Federal Acquisition Regulation Site*, *supra* note 15 (listing the Federal Acquisition Regulations that all contractors must comply with when selling and buying from the government); Gallacher, *supra* note 81 (describing the DFAR rule that controls research and development spending).

[119] *See* Wetterauer, *supra* note 39 (listing the amount of representation and certification requirements a contractor has to comply with). A contractor must have a NAICS, CAGE, and DUNS code to buy or sell with the U.S. government or another contractor. *See also* EXECUTIVE OFFICE OF THE PRESIDENT OFFICE OF MANAGEMENT AND BUDGET, North American Industry Classification System, at 77 (2017) (implying that these certifications are necessary to identify the size, location, revenue, etc. of a contractor).

[120] *See* 15 USC §645(d)(2013) (highlighting the statute that punishes contractors for misrepresenting themselves as small businesses just to be awarded a contract); *Supporting Small Businesses*, *supra* note 86 (introducing the Obama administration's initiative to award small contractors with defense contracts to compete in a defense industry dominated by larger contractors). *But see* Phillip G. Bail Jr, *supra* note 87 (explaining how large contractors are incentivized to misrepresent themselves to fit within the small businesses initiative to maintain their pre-existing contracts).

[121] *See* ManTech Advanced Systems International, Inc., B- 255719.2, 94-1 CPD P 326, at *1 (Comp. Gen. May 11, 1994) (speculating that Raytheon fraudulently misrepresented the amount of readied personnel available to provide services on the first day of the contract performance); *see also* Matter of ManTech Field Engineering Corporation, 1992 WL 70971, at *1 (Comp. Gen. Mar 27, 1992) (stating that

cess is fair because it allows small businesses to initiate and participate in the bid protest process which creates healthy competition amongst contractors and fosters fair dealing within the industry. [122]

Moreover, thousands of million-dollar transactions for products and services are still necessary to protect the U.S. and sustain the

---

the awardee of the contract lied on a government proposal about certain employee labor grades and the availability of such employees).

[122] *See e.g.* ManTech Advanced Systems International, Inc., B-255719 G.A.O. (1994), 1994 WL 242282, at *8 (highlighting the effective outcome of a bid protest and how it favors the contractor who protests a lost contract). The decision of this GAO case states:

> In sum, we find that Raytheon made misrepresentations that materially influenced the agency's evaluation of its proposal. We recommend that the Army recompete its requirements for the TROJAN electronic communications and reconnaissance system and, if a firm other than Raytheon is selected for award, terminate Raytheon's contract for the convenience of the government and make award to that firm, if otherwise eligible.

Id. See also Matter of ManTech Field Engineering Corporation, B-245886 G.A.O. (1992), 1992 WL 70971, at *3 (showing court's recommended course of action against the contractor that made misrepresentations in its bid proposal). The decision of this GAO case states:

> As a consequence of SEMA's failure to ascertain whether its proposed personnel were in fact available, the agency made its determination to award the contract to SEMA based on outdated, inaccurate information. We recommend that the agency reopen negotiations and call for a new round of BAFOs. If an offeror other than SEMA is then selected for award, we recommend that SEMA's existing contract be terminated.

Id. See also BID PROTESTS AT GAO: A DESCRIPTIVE GUIDE , *supra* note 61, at 1, 5-6 (discussing the history behind bid protests and how disputes are resolved by an "objective, independent, and impartial forum" that issues binding precedent); *The Antitrust Laws*, FED. TRADE COMMISSION (Mar. 7, 2018), *archived at* https://perma.cc/9NJJ-Z2F4 (explaining the three core federal antitrust laws: the Sherman Antitrust Act, the Federal Trade Commission Act, and the Clayton Act that preserve "free and unfettered competition").

economy because such transactions provide contractor jobs and bolster an already formidable military arsenal. [123] Additionally, if increased defense sales ever lead to leaked proprietary information, then cyber incident reporting regulations will enforce procedures to effectively handle such unauthorized disclosures. [124] Yet, despite President Trump's attempts to reduce contract prices of DoD transactions on essential military aerospace products such as the F-35 fighter jets, the DoD will continue to buy such products at a lower price to continue to strengthen the military and protect the nation.[125]

Furthermore, although contractor personnel took pay cuts due to decreased DoD expenditures, such as union workers at Sikorsky Aircraft, the DoD will not be deterred from continuing to purchase

---

[123] *See* 22 U.S.C.A §2751 (recognizing the importance for the United States and other countries to continue to engage in sales for defense equipment to maintain peace and security for the country's social, economic, and political progress). Further, this statute encourages countries to trade with each other to, "further the objective of applying agreed resources of each country to programs and projects of cooperative exchange of data, research, development, production, procurement, and logistics support to achieve specific national defense requirements and objectives of mutual concern." *Id. See also* O'Hanlon, *supra* note 89 (providing a perspective on R&D and how investing in R&D can help the economy with innovation and new technology).

[124] *See* § 252.204–7012(c) (providing the processes and requirements behind a cyber-incident reporting regulation); *see also* § 52.204–21(b) (setting forth the "cyber incident reporting" requirement); Zapotosky & Nakashima, *supra* note 57 (stating the facts of a case that lead to an arrest of a contractor employee who disclosed proprietary information).

[125] *See* Radelat, *supra* note 89 (pointing out how the Trump Administration reduced the contract price of F-35 fighter jets by $728 million). President Trump's latest initiative of reducing DoD expenditures occurred with the procurement of F-35 fighter jets. *Id.* The article states:

> In December Trump said the cost of the F-35 was "out of control." Earlier this month, he boasted of "the massive cost reductions I have negotiated on military purchases," and said he had extracted general promises to cut costs on the F-35 and on Boeing's new Air Force One after meetings with the chief executive officers of Lockheed Martin and Boeing.

Id.

necessary military products such as the Navy's CH-53K King Stallion helicopters.[126] Moreover, despite reduced contract prices, President Trump still plans to increase the DoD's budget in the future to have the capital necessary to acquire a multitude of military products and services at a more affordable price.[127]

More importantly, the military is starting to use encryption software in their unmanned aerospace products which is why reducing expenditures for such products will be harmful to the government rather than fiscally beneficial.[128] For example, necessary programs such as the Navy's Triton program are innovative programs that embed cyber capabilities into Unmanned Aerial Vehicles that are deployed and used to transmit signals to personnel on the ground. [129] Such a program enhances the U.S. military's capability and is one of the many necessary cyber programs that should continue to be maintained by the U.S. government.[130] Ultimately, the increased demand for cyber products in Aerospace and other sectors of the defense industry will lead to additional contract sales between the contractor and customer so that the American government and military can effectively compete in a globalized cyber world. [131]

---

[126] *See* Torres Ocasio, *supra* note 89 (discussing how the effects of reduced DoD expenditures have prompted contractors to reduce the pay of personnel who build military products). Sikorsky Aircraft, recently bought by Lockheed Martin, reduced union-worker salaries as a result of reduced contract prices for Navy Helicopters. *Id.*

[127] *See* Pramuk, *supra* note 92 (opining that President Trump will prioritize military spending in the new fiscal year by increasing the DoD's budget and decreasing all other federal agency budgets). Although some military contract prices have been reduced, the overall military budget will increase along with stock prices of major defense contractors who specialize in cyber products and other large military programs. *Id.*

[128] *See* Eckstein, *supra* note 77 (illustrating how the capabilities within the triton program represents a "significant milestone" and will be considered a multi-intelligence reconnaissance aircraft that promotes a man-machine teaming effort).

[129] *See* Eckstein, *supra* note 77 (describing the sensory capabilities of the UAVs within the Triton program).

[130] *See* Eckstein, *supra* note 77 (explaining the excitement behind launching the first squadron of Triton UAVs and how the launch is an innovative "milestone").

[131] *See* Insights, *supra* note 84 (describing how increased security threats have led to increased defense expenditures for modern weapons revolving around cyber). Deloitte reported that:

V. Conclusion

The strategy behind warfare will still continue to evolve, and such evolutions will be accompanied by innovative technology equipment used to attack and defend computer networks.[132] At some point, 'cyber' will be the most heavily requested style of equipment used by military forces throughout the world. Ultimately, artillery attacks will decrease, while computer network attacks will increase. Therefore, R&D contracts are more prevalent than ever because militaries recognize the need to innovate and adapt with new forms of technology to keep up with new forms of warfare.[133] Additionally, innovation requires increased expenditures to build new equipment. Therefore, it is expected that President Trump's request to increase the DoD budget is motivated by a need to develop new forms of cyber equipment necessary to prepare the U.S. for an age of computer warfare.[134]

> Defense budgets in the US, United Kingdom, France, Japan, several Middle Eastern countries, and other nations are increasing at a time when national security threats are being heightened with governments equip their armed forces with modern defense weapons platforms and next-generation technologies, including cyber, intelligence gathering, defense electronics, and precision strike capabilities.

Id.

[132] *See* Dinnis, *supra* note 23, at 22 (opining how the military's adoption of high technology equipment will improve the quickness and efficiency of contingency operations).

[133] *See* Gallacher, *supra* note 81 (illustrating the necessity of research and development contracts to foster innovation).

[134] *See* Pramuk, *supra* note 92 (highlighting President Trump's plan to increase the DoD budget to provide military forces with whatever resources they need).