REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
04-04-2018	Master of Military Studies Research Paper	September 2017 - April 2018

4. TITLE AND SUBTITLE

OVERSIGHT OF THIRD PARTY LOGISTICS PROVIDERS: THE MISSING INGREDIENT OF EXPORT CONTROL REFORM

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Mark T. McGlinchey

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Same as #7.

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT

Third party logistics providers (3PLs) constitute an important yet poorly regulated space in the US and global economy, which provide a means through which illicit actors route export restricted goods to prohibited end users. Authorities currently do not have a full quantitative understanding of the problems posed by 3PLs. This problem can be fixed by 1.) increased resourcing of already existing oversight agencies, initiatives and programs (OAIPs) with the requirement to increase focus on 3PLs; 2.) the establishment of a National Intelligence Mission Manager for Technology Security under the Office of the Director of National Intelligence; and 3.) the establishment of a new suspicious activity reporting (SAR) regime aimed solely at 3PL firms.

15. SUBJECT TERMS
export control, third party logistics, freight forwarders, non-vessel operating common carriers, illicit exports, export enforcement, t

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
Unclassified					Marine Corps University CSC
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UU	44	**19b. TELEPHONE NUMBER** *(include area code)*
Unclassified	Unclassified	Unclassified			(703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE: Oversight of Third Party Logistics Providers: The Missing Ingredient of Export Control Reform

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: Mark T. McGlinchey, U.S. Immigration and Customs Enforcement

AY 17-18

Mentor and Oral Defense Committee Member: Francis H. Marlo
Approved: [signature]
Date: 4 April 2018

Oral Defense ~~Committee~~ Member: Paul D. Gaupp
Approved: [signature]
Date: 4 April 2018

[signature] LT.COL. H. R. BRANNON
04 APRIL 2018

Executive Summary

Title: Oversight of Third Party Logistics Providers: The Missing Ingredient of Export Control Reform

Author: Mark T. McGlinchey, U.S. Immigration and Customs Enforcement

Thesis: Third party logistics providers (3PLs) constitute an important yet poorly regulated space in the US and global economy, which allows for loop holes through which illicit actors route export restricted goods to prohibited end users. This problem can be fixed by 1.) increased resourcing of already existing oversight agencies, initiatives and programs (OAIPs); 2.) the establishment of a National Intelligence Mission Manager for Technology Security under the Office of the Director of National Intelligence; and 3.) the establishment of a new suspicious activity reporting (SAR) regime aimed solely at licensed 3PL firms.

Discussion: 3PLs fulfill a vital function in international trade because they facilitate the movement of goods worldwide on behalf of both importers and exporters. The US government currently does not have a full quantitative understanding of the problems posed by 3PLs and the extent to which they are leveraged by proliferation agents of concern. It is apparent, however, through qualitative analysis of historical case data that lack of transparency in the transport sector is known and exploited by criminals engaged in various forms of illicit trade. This creates a gap in various enforcement mechanisms. The existing OAIPs set up to identify and investigate export control circumvention are relying on intelligence that is inadequate and does not relate to activity of 3PLs in the United States and transit countries of concern. In order to strengthen the overall export control system and counter-proliferation efforts, the government needs to more closely monitor 3PLs via regulatory, investigative, and intelligence means.

Conclusion: There are ways and means through which the export control community, in coordination with the intelligence community and industry, can more effectively identify, investigate, prosecute, and block illicit actors of concern.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Figures and Tables

Page

Table of Contents

Page

REPORT DOCUMENTATION PAGE		FORM APPROVED - - - OMB NO. 0704-0188	
PUBLIC REPORTING BURDEN FOR THIS COLLECTION OF INFORMATION IS ESTIMATED TO AVERAGE 1 HOUR PER RESPONSE, INCLUDING THE TIME FOR REVIEWING INSTRUCTIONS, SEARCHING EXISTING DATA SOURCES, GATHERING AND MAINTAINING THE DATA NEEDED, AND COMPLETING AND REVIEWING THE COLLECTION OF INFORMATION. SEND COMMENTS REGARDING THIS BURDEN ESTIMATE OR ANY OTHER ASPECT OF THIS COLLECTION OF INFORMATION, INCLUDING SUGGESTIONS FOR REDUCING THIS BURDEN, TO WASHINGTON HEADQUARTERS SERVICES, DIRECTORATE FOR INFORMATION OPERATIONS AND REPORTS, 1215 JEFFERSON DAVIS HIGHWAY, SUITE 1204, ARLINGTON, VA 22202-4302, AND TO THE OFFICE OF MANAGEMENT AND BUDGET, PAPERWORK REDUCTION PROJECT (0704-0188) WASHINGTON, DC 20503			
1. AGENCY USE ONLY (*LEAVE BLANK)*	2. REPORT DATE 04-04-2018	3. REPORT TYPE AND DATES COVERED *Master of Military Studies Research Paper*	
4. TITLE AND SUBTITLE OVERSIGHT OF THIRD PARTY LOGISTICS PROVIDERS: THE MISSING INGREDIENT OF EXPORT CONTROL REFORM		5. FUNDING NUMBERS *N/A*	
6. AUTHOR(S) Mark T. McGlinchey			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) *USMC COMMAND AND STAFF COLLEGE* *2076 SOUTH STREET, MCCDC, QUANTICO, VA 22134-5068*		8. PERFORMING ORGANIZATION REPORT NUMBER N/A	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) *SAME AS #7.*		10. SPONSORING/MONITORING AGENCY REPORT NUMBER: N/A	
11. SUPPLEMENTARY NOTES *N/A*			
12A. DISTRIBUTION/AVAILABILITY STATEMENT *NO RESTRICTIONS*		12B. DISTRIBUTION CODE *N/A*	
ABSTRACT *(MAXIMUM 200 WORDS)* Third party logistics providers (3PLs) constitute an important yet poorly regulated space in the US and global economy, which provide a means through which illicit actors route export restricted goods to prohibited end users. Authorities currently do not have a full quantitative understanding of the problems posed by 3PLs. This problem can be fixed by 1.) increased resourcing of already existing oversight agencies, initiatives and programs (OAIPs) with the requirement to increase attention to 3PLs; 2.) the establishment of a National Intelligence Mission Manager for Technology Security under the Office of the Director of National Intelligence; and 3.) the establishment of a new suspicious activity reporting (SAR) regime aimed solely at 3PL firms.			
14. SUBJECT TERMS (KEY WORDS ON WHICH TO PERFORM SEARCH) export control, third party logistics, freight forwarders, non-vessel operating common carriers, illicit exports, export enforcement, technology transfer, International Trafficking in Arms Regulations, ITAR, Commerce Control List, CCL, Export Control Reform, proliferation, counter-proliferation, procurement networks, Iran, North Korea, China, Russia, international terrorist organizations		15. NUMBER OF PAGES: 44 16. PRICE CODE: N/A	
17. SECURITY CLASSIFICATION OF REPORT *UNCLASSIFIED*	18. SECURITY CLASSIFICATION OF THIS PAGE: *UNCLASSIFIED*	19. SECURITY CLASSIFICATION OF ABSTRACT *UNCLASSIFIED*	20. LIMITATION OF ABSTRACT N/A

Preface

This paper is a modest effort to call attention to a tactic used to circumvent strategic trade controls. Put another way, this tactic is a symptom of a larger problem. The larger problem is the outbound proliferation of weapons and dual use goods that can be used to make weapons to strategic rivals, rogue states, and transnational terrorists. 3PLs are simply a link in the chain through which this illicit trade occurs. If this paper only increases situational awareness on the inherent vulnerabilities existing within this link in supply chains, it will have achieved its main purpose. A secondary purpose is to recommend solution sets with which to more directly correct the problem. A tertiary purpose is to increase awareness on the domestic side of counter-proliferation (export controls and enforcement) and its place at the intersection of both national security and economic competitiveness and how these two priorities need to be balanced.

First and foremost, I wish to acknowledge the invaluable guidance and assistance received from my mentor at USMC Command and Staff College, Dr. Frank Marlo. I also received substantial assistance and suggestions for improvement from Keith Maly, my unit chief at ICE and a retired US Navy intelligence officer. Additionally, Kathleen McGlinchey, a retired English teacher and paternal aunt, provided excellent advice on grammar and punctuation. Andrea Hamlen at the Grey Research Center's Leadership Communications Skills Center provided additional grammar, style, and punctuation proofreading assistance. Thank you also to Professor Bert Chapman of Purdue University, a subject matter expert on the history of US export controls, for providing valuable guidance on pertinent citable sources. Most importantly, thanks to my beautiful wife Inna for her love and patience while I spent so much time away from home researching, writing, and re-writing. Thank you to all. Any imperfections, oversights, or errors within are solely my own.

Introduction

> *"Proliferators spearheading these procurement networks are able to quickly locate products for sale anywhere in the world… [and] communicate that information via email to their middlemen overseas and direct them to specific US suppliers. These foreign middlemen… work in conjunction with freight forwarders who at their instruction remove and replace the inbound shipping records with outbound shipping records to facilitate the transshipment of the goods to prohibited end-users."*
>
> *-Ryan P. Fayhee, Acting Deputy Chief, National Export Enforcement Coordinator, Department of Justice*[1]

The overarching goal of US export control reform is to simplify the complex system for controlling the exportation of strategically significant[i] technologies in order to prevent their diversion to key proliferation actors of concern (e.g. Iran, North Korea, China, Russia, and transnational terrorist organizations). The focus of this paper lies at the intersection of one means proliferation actors can use to illicitly obtain export restricted technologies and the inadequacy of the proposed reform of the system set up to prevent proliferation actors from obtaining said technologies. Qualitative analysis of export control reform literature and unsealed court records indicate a lack of policy attention to entities in the supply chain that are able to either help or hinder adversary circumvention of export controls. Is export control reform, as defined today, adequately accounting for the complexity of the system it is charged with controlling? What can government do to increase scrutiny and oversight regarding supply chain intermediaries that provide logistics services as a third-party? Third party logistics firms (3PLs) include, but are not limited to, freight forwarders, non-vessel operating common carriers, and customs brokers. 3PLs

[i] Strategically significant technologies, broadly defined, include those which have the potential to significantly strengthen adversary military capabilities going forward. Based upon the Defense Security Service's industrial base technology list (IBTL), it includes but is not limited to the following categories of technology: nuclear, chemical, biological, electronics, C4, software, aeronautic systems, radars, space systems, marine systems, acoustic sensors, ground systems, armament and survivability systems, energetic systems, manufacturing equipment and processes, optics, lasers, directed energy, signature control systems, nanotechnology, synthetic biology, cognitive neuroscience, computational modeling of human behavior, and quantum systems. These technologies are strategically significant and export controlled.
(IBTL: https://www.cdse.edu/documents/cdse/CI-JobAidSeries-IBTL.pdf)

constitute a poorly regulated space in the US and global economy, that illicit actors exploit to ultimately deliver strategically significant technology to prohibited end users. This thesis will primarily demonstrate that in order to strengthen the export control system, the government needs to more closely monitor 3PLs. The secondary purpose is to briefly review possible solutions the export control community can employ to more effectively protect technology and disrupt the flow of such items to prohibited end users via multi-disciplinary techniques.

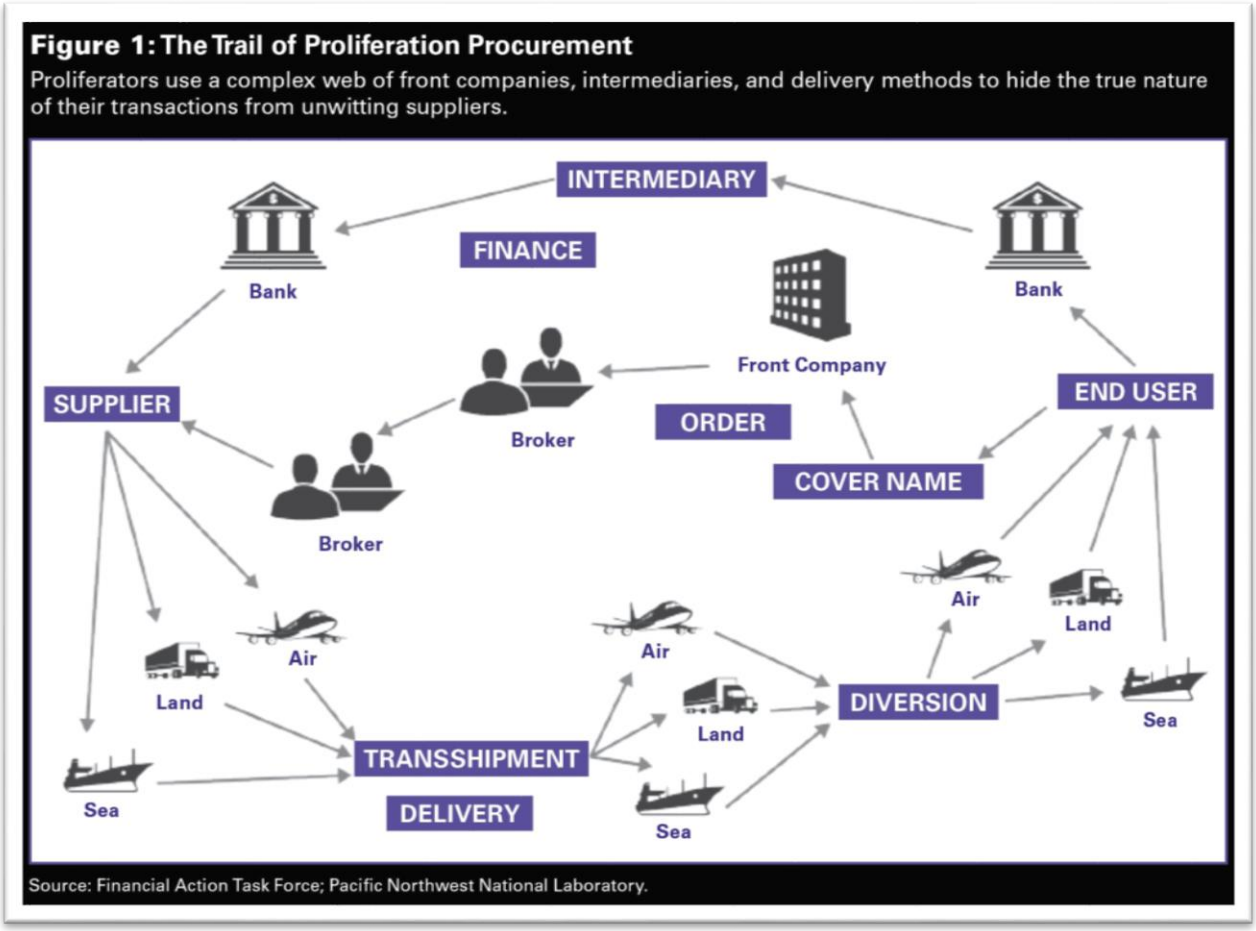
Export controls are laws[ii] and multilateral regimes[iii] that govern the distribution of strategically important technology, services, and information for reasons of foreign policy and national security. The principle mechanism for entities to demonstrate compliance with these controls is the export license. However, export licenses can be obtained fraudulently. Illicit actors operate within this system to acquire and move export-restricted technologies to US adversaries. This form of illicit trade has strategic consequences, and can both minimize the technological advantage that the US military currently enjoys on the battlefield as well as adversely affect US economic competitiveness in world markets.

The figure below from the Pacific Northwest National Laboratory illustrates the potentially complex nature of supply chains in these transactions.[2] The range of means illicit actors use may be as simple as skipping the procurement of an export license altogether or as complex as acquiring a fraudulent license via a front/shell company. Additional 3PL entities, front companies, and brokers may be deliberately inserted into the supply chain to further

[ii] The four main export control laws within the US Code are: 1.) the Arms Export Control Act (22 USC 2778); 2.) the Export Administration Act (50 USC 2411-2420); 3.) the International Emergency Economic Powers Act (50 USC 1705); and 4.) Smuggling Goods from the United States (18 USC 554).

[iii] The five primary multilateral export control regimes are: 1.) the Zangger Committee (nuclear); 2.) the Nuclear Suppliers Group (nuclear); 3.) the Australia Group (chemical and biological); 4.) the Missile Technology Control Regime (missiles); and 5.) the Wassenaar Arrangement (dual use goods and conventional arms).

obfuscate the ultimate destination of restricted technology. Oftentimes, suppliers are unwitting as to the identity of the true end user.



Source: Andrew Kuzrok and Gretchen Hund, Arms Control Today, June 2, 2014.

US Export Control System History, Overview, and Impetus for Reform

Just as the responsibility to control restricted technology is spread across the US Code and international agreements, the authority to do so is also distributed across the federal government. Competing responsibilities and overlapping authorities make the business of US

export control inherently difficult and ineffective.[iv] To understand the 'as is' system of today, a brief historical review of export controls is in order.

Pre-Cold War Era

By way of historical context,[v] the tasks, responsibilities, and practices of the US export control system have their early origins in laws passed during wartime. Embargos enacted in 1807 and 1809 in response to the Napoleonic Wars between Great Britain and France resulted in the Embargo Act of 1813 enacted during the War of 1812. The embargos and acts from this time period were very broad, at one point effectively banning US ships from trading (both exports and imports) with all countries, not just Britain and France. While impacting the targeted countries, some historians believe they were equally or more harmful to the US economy, particularly in the northeastern states. Both Jefferson and Madison envisioned the measures as a form of peaceful coercion, which would effectively punish European belligerents, change the British policy of impressment, and keep the US out of war.[vi] During World War I, the 1918 Trading with the Enemy Act prohibited selling materials of military significance to Germany and its allies for the duration of the war. As President Woodrow Wilson explained, in the *Official*

[iv] For a brief introduction to the inherent difficulties in the interagency system as applied to export controls, read chapter 3 of The National Academy's *Export Control Challenges Associated with Securing the Homeland*, entitled "*The Interagency Process For Export Controls*."; National Academies Press, *Export Control Challenges Associated With Securing the Homeland* (Washington DC: National Research Council of the National Academies, Committee on Homeland Security and Export Controls, 2012), 33-46, https://www.nap.edu/read/13369/chapter/6.

[v] For a more complete background of Export Control history, recommend reading the definitive work on this subject, Bert Chapman's *Export Controls: A Contemporary History*. Another worthwhile study is Richard T. Cupitt's *Reluctant Champions: US Presidential Policy and Strategic Export Controls*.

[vi] For a more complete background of the 1812 era embargos, recommend reading Reginald Horsman's *The Causes of the War of 1812*, particularly Chapter 7 entitled *The Failure of the Embargo*. The export controls from this time were overly broad, poorly enforced, of limited duration, and had no discernible impact on British war fighting capabilities. Though largely symbolic, they still set an important precedent for the use of trade restrictions in US foreign policy.

Bulletin,[vii] the new export licensing procedures were to be "as simply organized and administered as possible, so as to constitute no impediment to the normal flow of commerce."[3]

Cold War Era

The bulk of permanent US export control laws and multi-lateral export control regimes in existence today, however, have their origins in the Cold War. The basis of the controls, as explained by Hungarian Trade Office authority Noemi Mintal, was a common understanding among NATO member states that "any strategic advantage [they] held over the Soviet bloc countries was [greatly dependent upon] its technological superiority."[4] The US and its allies maintained technological superiority, in part, through the Coordinating Committee for Multilateral Export Controls (CoCom) which strictly regulated the export of military use and dual use technologies to the Soviet Union, Warsaw Pact nations, the People's Republic of China, and other Communist nation-states. Similar to most national security related policies and organizations, the export control system's justification lies in preserving and building strategic advantage while simultaneously mitigating present and future threats.

The Strategic Context of Technology and Export Controls

Export controls are a means towards the end of reduction of future threats; they attempt to deny to threat countries the building blocks of strategic technological advantage. French Army General and military strategist André Beaufre best summarized the strategic context behind the policy as follows:

> A gigantic technological race is in progress…[i]t is a form of indirect attrition; instead of destroying enemy resources, its object is to make them obsolete, thereby forcing on him enormous expenditure…A silent and apparently peaceful war is therefore in progress, but it could *be a war which of itself could be decisive.*[5]

[vii] The Committee on Public Information published the *Official Bulletin* and was an independent agency set up to influence public opinion in favor of US participation in World War I. Wilson anticipated the new export controls would give rhetorical support to isolationist opponents of the war effort. Wilson viewed the *Official Bulletin* as a means to communicate his views and policy goals directly to the American public and circumvent newspapers of the day.

Strategists such as Beaufre and his contemporaries believed it was in the strategic interest of a technologically superior state to restrict the export of militarily significant technologies in such a manner that they would be less likely to end up in the hands of enemies and strategic rivals.

Functional Group Overview of the US Export Control Community

Table 1 logically groups the export control community into five separate segments. It provides brief descriptions of each functional group and identifies the principal executive branch departments and agencies involved with the group.

Table 1: Five Functional Groups Within the Export Control Community	
Regulatory and Licensing Group	Accepts export license applications and issues or denies as appropriate. Promotes US exports and trade while simultaneously providing regulation and oversight through the export licensure process. (Main Players: State, Commerce, and Treasury, allied counterparts)
Law Enforcement Group	Investigates and arrests illicit actors and seizes export restricted outbound goods intended for prohibited end users. (Main Players: ICE-HSI, CBP, Commerce, FBI, Defense, allied counterparts)
Intelligence Group	Gathers, analyses, and disseminates information on procurement agents and networks. Identifies what technologies procurement agents are targeting and what tactics they are employing to circumvent export controls. (Main Players: 16 Agencies of the US Intelligence Community, intelligence personnel in non-title 50 agencies, allied counterparts)
Prosecutorial and Judicial Group	Puts the suspects arrested by the law enforcement community on trial and sentences guilty parties. Coordinates extraditions of suspects with the diplomatic community. (Main Players: Justice, US District Courts, allied counterparts)
Diplomatic Group	Negotiates and monitors international treaties and multilateral agreements that affect management and enforcement of export controls. Also evaluates visa applicants for deemed export concerns prior to issuance of student, work, and travel visas. Diplomacy also includes economic sanctions, which are broad-based export controls. (Main Players: State, Treasury, allied counterparts)

Source: William Argue, HSI Authorities (Homeland Security Investigations Counter-Proliferation Investigations Training Seminar) June 15-19, 2015

The list of departments and agencies above is not all inclusive. Other agencies involved with export controls include the Department of Energy, the Nuclear Regulatory Commission, Food and Drug Administration, Drug Enforcement Administration, Defense Security Service, Defense Criminal Investigative Service, Naval Criminal Investigative Service, Air Force Office of Special Investigations, the US Postal Service, the Census Bureau, the Federal Maritime Commission, and several others. In addition, private industry and non-governmental organizations also have vital roles to play.

SECDEF Gates' 2010 Speech to Business Executives for National Security

Secretary of Defense Robert Gates, in a 2010 speech to Business Executives for National Security, argued export control reform was needed for national security, broadly defined to include competitiveness of US industry in a globalized economy. America requires a reformed system, he insisted, that:

1. increases interoperability and trust with close allies;
2. enhances and preserves the US industrial base by eliminating the incentives allied defense manufacturers have for building systems with intentionally designed out US origin content (with the intent of avoiding the current US export control process entirely);
3. and also allows for more selective and explicit prioritization of technologies of strategic concern.

What Secretary Gates meant with the third sub-set argument was that the US export control system should become more narrowly focused, and thus made more effective. In short, Gates

said, America should evolve to a system where "higher walls are placed around fewer, more critical items."[6]

The Four Singulars

The most recent export control reform effort, as envisioned by the Obama Administration in 2010, has the goal of transforming the US export control system into one based on "four singles." First, is *a single export control licensing agency* for dual-use goods and munitions exports--as well as Treasury-administered sanctions and embargoes. Second, is *a single unified control list* which would consolidate the Export Administration Regulations (EAR),[viii] the International Traffic in Arms Regulations (ITAR),[ix] and Office of Foreign Asset Control (OFAC)[x] sanction/embargo regulations. Third, is the establishment of *a single integrated information technology (IT) system.* Fourth, is the establishment of *a single primary enforcement coordination agency*.[7]

Export Control Reform Current Status

At the end of the Obama Administration, the US government had achieved some partial progress on the singulars. Regarding lists, the Departments of State and Commerce, in coordination with other stakeholders, have largely eliminated the redundancy that had always existed between the existing lists. Many export controlled items on the simple and highly restrictive ITAR United States Munitions List (USML) governing military use being moved to

[viii] EAR is a dual-use control list which regulates the export of dual use items which are designed for commercial purposes, but which could have military uses. EAR requires that information and material listed on the Commerce Control List (CCL) may only be exported with authorization (an export license) from the Department of Commerce. The latest versions of EAR and CCL can be found in the code of federal regulations under 22 CFR 730-774 and 15 CFR 774.

[ix] ITAR is a military use control list which regulates the export of defense-related articles and services on the US Munitions List. ITAR requires information and material pertaining to defense related technologies may only be exported with authorization (an export license) from the Department of State. The latest version of ITAR can be found in the code of federal regulations under 22 CFR 120-130 as well as the State Department's website (https://www.pmddtc.state.gov/regulations_laws/itar.html).

[x] OFAC regulations are a prohibited end-user control list used to prohibit trade with designated entities in support of US national security and foreign policy objectives. OFAC sanction and embargo regulations dictate trade with certain countries and individuals/firms within certain countries can only occur with authorization (an export license) from the Department of Treasury.

the more complex and less restrictive EAR Commerce Control List (CCL).[xi] Regarding enforcement coordination, the Export Enforcement Coordination Center (E2C2) was established via Executive Order in 2010 with the purpose of establishing a single primary enforcement agency. E2C2 has personnel from over 19 federal law enforcement, intelligence, and export licensing agencies and epitomizes the term "interagency." United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE-HSI) leads E2C2 and there are two Deputy Directors, one from the Department of Justice (FBI) and one from the Department of Commerce's Bureau of Industrial Security (BIS).[8] Regarding the single IT system, Department of Defense was designated the executive agent for the creation and maintenance of an integrated IT system, known as USEXPORTS, which includes information on sanctioned and denied entities and helps create, at the unclassified level, a shared common operating picture across the export control community.[xii] Regarding licensing, as of early 2018, there were still three primary export licensing agencies (Commerce, State, and Treasury).

Control Hawks versus the Run Faster Coalition

Ultimately, if further progress towards the four singulars is to happen, Congress and the President must produce reform legislatively. Unfortunately, there is a lack of consensus within the export control community regarding reform as it is currently conceived and being implemented. Many details of this reform process, and its anticipated effects on both national security and economic growth, are subject to debate and discussion. Hugo Meijer's 2016 book *Trading with the Enemy: The Making of US Export Control Policy Towards the People's*

[xi] The Department of State's Directorate of Defense Trade Controls (DDTC), which manages ITAR export license applications, has experienced a 55 percent decline in license processing volume since 2013 due to the transfer of several ITAR categories to CCL. In principle, this movement of goods towards the less restrictive list gets the US closer towards Gate's goal of a system of higher walls around fewer items.

[xii] In addition to increasing unity of effort and efficiencies, a single IT system could serve as a valuable analytical tool for criminal investigators and intelligence analysts.

Republic of China offers one of the most definitive explications of this debate. Meijer presents a two-sided argument that labels the export control reform skeptics as "control hawks,"[xiii] who prefer to err on the side of restricting technology flows. Control hawks argue the older model used against the former Soviet Union needs only slight modifications and still has utility against peer competitors such as China and Russia, as well as rogue states such as Iran and North Korea. Meijer labels the other side the "Run Faster Coalition,"[xiv] who argue America's only hope for strategic dominance in the post-Cold War globalized world is to have a more permissive export control policy. A freer flow of goods and a full embrace of off-the-shelf technologies, they maintain, is the best way to make sure America and her key allies can collaborate and out-innovate strategic peer competitors and maintain and improve technological advantage over rogue states. A good way to summarize the run faster coalition view is the maxim, "it is wiser to advance the leader than to seek to delay the pursuer."[9] Both sides in this debate have valid points and counterpoints. Both also tend to ignore the role 3PLs can play in export control circumvention and have not seen it for what it is: a systematic vulnerability in need of mitigation.[10]

3PLs as Stakeholders in Trade Security

Firms known as 3PLs play a vital role in international trade because they facilitate the movement of goods worldwide on behalf of importers and exporters. They are also known as freight forwarders, non-vessel operating common carriers, ocean freight forwarders, ocean transportation intermediaries, indirect air carriers, air shippers, forwarding agents, parcel

[xiii] Two representative works for the Control Hawks can be found in Andrea Stricker and David Albright's 2017 study entitled *US Export Control Reform: Impacts and Implications for Controlling the Export of Proliferation-Sensitive Goods and Technologies* and David R. Fitzgerald's 2014 article entitled *Leaving the Back Door Open: How Export Control Reform's Deregulation May Harm America's Security.*

[xiv] Two representative works for the Run Faster Coalition are the National Academy Press's 2009 study, *Beyond 'Fortress America': National Security Controls on Science and Technology in a Globalized World* and Brandt Pasco's 2014 article in Harvard Law School's National Security Journal entitled *The Case for Export Control Reform, and What it Means for America.*

forwarding centers, mail forwarding companies, cargo consolidators, and customs brokers. Both government and industry stakeholders use these terms interchangeably despite some fine distinctions amongst these entities.[xv] For brevity and simplicity, this paper will use the term 3PL to describe all such firms.[11] A high percentage of international containerized trade uses the services of a 3PL at least once along the supply chain (especially if the goods undergo transit or transshipment).[xvi] In addition to dealing with customs authorities, preparing documentation, and identifying efficient shipping routes, 3PLs also buy and sell space aboard cargo ships and airplanes. The 3PL is the expeditor, interfacing with all necessary government agencies and companies involved in international transportation of cargo to its ultimate destination. Competition in this market is intense, profit margins are increasingly thin, and illicit actors view the situation as a vulnerability to be exploited. The current regulatory framework for the 3PL industry is inadequate and relatively easy for bad actors to circumvent. This lax regulatory structure inadvertently provides a means for criminal enterprises to undermine anti-money laundering controls. Moreover, the industry itself has an overall lack of transparency due to the low barriers for entry and large number of small and medium sized enterprises operating as 3PLs.[12]

By way of background, US exports are on the rise. According to *Fortune* magazine, as of June 2017, US exports of goods rose 1.2 percent to 194 billion dollars, the highest level since

[xv] One basic distinction to be aware of is freight forwarders simply move cargo from one point to another. Third-party logistics providers move, store, and process inventory, and in doing so, may provide traditional forwarder services. Freight forwarders (also commonly known as non-vessel operating common carriers) offer a more limited and traditional service but are generally lower cost. 3PL is the label of choice for this paper because it is the more all-encompassing umbrella term which captures the entire industry sector.

[xvi] According to shippingandfreightresource.com, transit and transshipment are defined as follows: "Transshipment is the act of off-loading a container from one ship (generally at a hub port) and loading it onto another ship to be further carried to the final port of discharge…Cargoes which have been off-loaded at a port for transshipment are NOT allowed to exit the port by land or rail across international borders…unless they are declared as Cargo in Transit…Cargo in Transit is the movement of cargo discharged at a gateway seaport or originating from a country within a union (i.e. the European Union or African Union) across international borders to another country where the final destination is (generally) a landlocked country." https://shippingandfreightresource.com/transhipment-and-cargo-in-transit/

December 2014. 3PLs are a link in the chain (in addition to the importers, exporters, and carriers) which gets these goods to their final destinations. A 2014 study by the Stimson Center observed these firms are "increasingly utilized, evidenced by logistic service provider revenues increasing 7-16 percent annually" over the previous five years. The firms that facilitate movement of the world economy's goods are private in nature, the Stimson Center stated, but in their collective roles and impact are also "a public good that is shared across national borders," and a key component of critical infrastructure and international security.[13]

Quantitative Versus Qualitative Research on 3PLs

A survey of publicly available literature demonstrates a pronounced lack of quantitative research concerning export control circumvention using 3PLs. However, one can gain an appreciation for 3PL importance and insight into their role in illicit trade through qualitative research. A cursory analysis of the *Justice Department's Summary of Major US Export Enforcement, Economic Espionage, Trade Secret, And Embargo-Related Criminal Cases* and other pertinent government documents demonstrate multiple cases with 3PLs, both US-based and overseas, involved in illicit transactions. It would be a mistake to look at the Justice Department case summaries through a quantitative lens, as these publicly available data sets are not exhaustive and only represent the most egregious examples of export control circumvention. Appendix A contains a list of 15 pertinent criminal and administrative case summaries.[14]

The Role of 3PLs in the Supply Chain and Compliance Responsibilities

It is important to remember 3PLs are neither the manufacturers nor wholesalers of the goods shipped nor are they owners of the shipment. Typically, they are not listed as a US

Principle Party in Interest[xvii] (USPPI) in the Electronic Export Information form[xviii] (EEI). These firms are reliant on information or documentation supplied by another party in the transaction, often their customer—and possibly, a manufacturer or wholesaler with which they have no commercial relationship. 3PL customers can include exporters (i.e. USPPIs), other freight forwarders, customs brokers, airlines, shipping lines, the end user, or a representative of the end user. 3PLs are still legally responsible for following export control regulations. Concomitantly, this does not relieve the USPPI of their legal responsibilities. It is not an either/or proposition, since both the USPPI and the 3PL must work together to ensure compliance. Commerce's BIS website provides extensive guidance aimed at 3PLs outlining legal responsibilities[xix] and red flags[xx] of concern. Appendix B contains a more comprehensive list of pertinent red flags for these firms, derived from a Stockholm International Peace Research Institute report, and provides an outline of the myriad ways export control circumvention can happen via 3PLs. [15]

Regular Versus Routed Export Transactions

One distinction to be aware of in this area of trade is the difference between regular export and routed export transactions. In a regular export transaction, the USPPI hires the 3PL and tells it what and where to ship. A routed export transaction, however, occurs when the Foreign Principle Party Interest[xxi] (FPPI) selects their own US-based 3PL and provides them a power of attorney to act as the FPPI's agent and export the goods. In this instance, the 3PL has a

[xvii] The USPPI is the person or legal entity that receives the primary benefit, monetary or otherwise, from the export transaction. Generally, that person or entity is the US seller, manufacturer, or order party, or the foreign entity while in the United States when purchasing or obtaining the goods for export.

[xviii] An Electronic Export Information form (EEI) is required if a single commodity's value within a US export shipment exceeds $2,500. EEIs must be filed with the U.S. Census Bureau electronically through the Automated Export System (AES). EEI records are used by the US Census Bureau to compile trade statistics which are used by the export control community. EEIs were formerly known as Shipper's Export Declarations (SEDs).

[xix] BIS freight forwarder guidance: https://www.bis.doc.gov/index.php/documents/compliance-training/export-management-compliance/620-new-freight-forwarder-guidance/file

[xx] BIS list of red flags for freight forwarders: https://www.bis.doc.gov/index.php/documents/regulation-docs/411-part-732-steps-for-using-the-ear/file

[xxi] A Foreign Principal Party in Interest (FPPI) is the party abroad who purchases the goods for export or to whom final delivery or end-use of the goods will be made. This party may be the Ultimate Consignee. In may also be a 3PL.

heightened export control compliance role and legally becomes the exporter for EAR purposes. Here, the 3PL must apply for the export license. If the firm in question has a competent and law-abiding export compliance manager, all should go well. However, unsurprisingly, illicit actors of concern seeking to circumvent export controls on behalf of prohibited end users generally do not seek out 3PL firms with good compliance programs. An added difficulty arises with routed exports when the 3PL is dependent upon the US supplier (with which they have no commercial relationship) for the proper information with which to apply for an export license. In practice, this can and does lead to 3PLs submitting inaccurate and incomplete information for export licenses and results in export control violations. In some cases this is due to exporters deliberately and with criminal intent providing the 3PL erroneous information and in some cases it is due to exporter or 3PL unfamiliarity with export control law requirements to provide correct categorization of goods prior to application for the export license. How much of either is occurring now or has occurred historically would be a subject worthy of further study.[16]

Lack of Transparency

The central issue of concern with 3PLs is lack of transparency. One reaches this conclusion by means of comparison of the transport sector of the economy with the financial sector. The rule sets implemented domestically and internationally on financial institutions under the auspices of the Treasury Department, the Financial Crimes Enforcement Network (FinCEN), and the multilateral Financial Action Task Force (FATF), while not eliminating money laundering and terrorist financing, have certainly made it more difficult on the criminals and terrorists to move money. In the transport sector, there is no equivalent to Suspicious Activity Reports[xxii] to identify and track possibly suspicious outbound shipments. As Nikos Passas and

[xxii] Since 1996, under the Bank Secrecy Act, banks and financial institutions are required by law to file Suspicious Activity Reports (SARs) when they detect a suspicious transaction of $5,000 or more which could possibly involve money laundering or

Kimberly Jones observed, trade transactions using 3PLs are a means through which illicit actors can break up transactions, obfuscate the true nature of their business, and get around financial controls. Transnational criminal organizations have long used this practice as part of trade-based money laundering (TBML) - to move the illicit proceeds of crime, and very little prevents restricted technology procurement agents from also using the same techniques. Passas and Jones cite Non-Vessel Operating Common Carriers (NVOCCs) as a primary area of concern and conclude the "ease with which NVOCCs can evolve and operate in different ways constitutes a significant vulnerability."[17]

Mere Taxi Drivers?—the Viktor Bout Network

Some 3PL firms, implicitly or explicitly, do not see counter-proliferation as an obligation. The most notorious example from recent history is the Viktor Bout[xxiii] arms trafficking network. Bout was implicated in facilitating the violation of United Nations arms embargoes in the Democratic Republic of the Congo, Angola, Sierra Leone, Liberia, and several other countries during the nineties. Bout and his defenders long described his enterprise as nothing more than an air freight forwarder. In a 2002 interview, Viktor Bout's older brother and business partner, Sergei Bout, bluntly articulated this point of view:

> Imagine a taxi driver who is supposed to give a lift to a customer who asks him to take him to a certain location. But suddenly this taxi driver asks the customer what is in your suitcase? It is not my bloody business what my customer has in his trunk. I am a taxi driver, I am a carrier. I don't know what I carry. Maybe I carry a nuclear bomb. No one is informing me about it.[18]

terrorist financing. In 2016, approximately 960,000 SARs were filed by private financial institutions and submitted to FinCEN. Many money laundering criminal cases have their start with the initial submission of a SAR from private industry.

[xxiii] Bout and his international weapons trafficking activities were dramatized in a 2005 feature film entitled *Lord of War*. Another source of interest is the 2007 book entitled *Merchant of Death: Money, Guns, Planes, and the Man Who Makes War Possible* by Douglas Farah and Stephen Braun.

Besides transporting weaponry, Bout's firm routinely transported an assortment of mundane commodities such as food stuffs and humanitarian supplies. This mixing of licit and illicit trade was, in large part, what allowed him to operate unencumbered for so long. In 2011, a US District Court convicted Bout of conspiring to sell millions of dollars' worth of weapons to the Revolutionary Armed Forces of Colombia (FARC) – a terrorist organization. He is currently serving a 25 year prison sentence at a medium-security federal prison in Marion, Illinois.[19]

Ten Easy Pieces: Existing Oversight Agencies, Initiatives, and Programs (OAIPs)[xxiv]

There are several existing oversight agencies, initiatives, and programs (OAIPs) that have some form of oversight of 3PLs and concern themselves with security and counter-proliferation to varying degrees. Ten OAIPS having 3PLs or counter-proliferation in their purview include:

1. the Federal Maritime Commission, which licenses ocean transportation intermediaries, freight forwarders, and non-vessel operating common carriers operating in the US;
2. Project Shield America, which is ICE-HSI's industry outreach program;
3. Infragard, which is FBI's industry outreach program;
4. Commerce's industry outreach program;
5. Blue Lantern, which is the State Department's end-use check/verification program;
6. Sentinel, which is Commerce's end-use check/verification program;
7. Global Sentry, the Defense Security Cooperation Agency's end-use check program;
8. the State Department's Export Control and Related Border Security (EXBS) Program, which provides training to the Customs Services of allied countries;

[xxiv] A review of the literature shows a high number of studies and government programs concerned with domestic port security, clandestine nuclear attack in Homeland ports, as well as conventional bombing threats with a nexus to air cargo and air transport. While these low-probability high-impact threats are of concern to trade sector security broadly conceived, they are neither export control nor counter-proliferation focused and are outside the scope of this paper.

9. the Proliferation Security Initiative, which is a broad-based multi-national effort focused on WMD-related trafficking and interdiction worldwide;

10. and United Nations Security Resolution 1540, which requires all the world's nations to implement measures to prevent illicit actors from trading in, or acquiring, WMD as well as the dual use equipment for manufacturing and delivering WMD.

The intent of this overview of existing OAIPs is both to provide overall context on what is being done to prevent export control circumvention and to illustrate their broad-based nature. With the exception of the Federal Maritime Commission, which conducts perfunctory oversight in support of its licensing function, none of the OAIPs are specifically focused on 3PLs.

The Federal Maritime Commission[xxv]

The Federal Maritime Commission (FMC) is a regulatory agency that oversees and licenses the majority of 3PLs offering ocean transportation services in the US and grants licenses to firms meeting their requirements. As of the writing of this paper, there are approximately 6,500 firms licensed or registered (of which approximately 4,500 are licensed)—75 percent of the 6,500 total are located in the US. Foreign firms conducting business in US ports do not require a license from FMC but may choose to obtain one to gain lower bond or insurance rates. To obtain license approval, FMC performs basic background checks for applications on the individuals who own or manage the 3PL as well as the firm itself using the Accurint[xxvi] database. Additionally, license applicants need to provide three references with first-hand knowledge of their ability to move cargo from one country to another. They also must have three years of industry experience. On average, the FMC approves approximately 75 percent of all 3PL license

[xxv] For more details on the Federal Maritime Commission and the latest version of their Ocean Transportation Intermediary list, go to: https://www2.fmc.gov/oti/NVOCC.aspx.

[xxvi] Accurint is an open source commercial database used by lawyers, financial services, insurance, telecommunications, and retail businesses in addition to state and federal law enforcement agencies. It contains billions of data records on individuals and businesses, as well as proprietary data-linking methods.

applications. Most license applicants not approved are unable to provide acceptable references. Non-renewal of bonds is the FMC's most common reason for delisting licensees and all licensees must carry commercial insurance (have sufficient bond). The FMC's licensing bureau reports approximately10 percent of the companies handle 90 percent of the imports and exports and approximately 90 percent of the FMC licensed firms are mid-sized or small businesses.[20]

Industry Outreach

Integral to the effort of identifying and investigating bad actors of counter-proliferation concern is law enforcement industry outreach. Industry outreach is a vital source of investigative leads and many successfully prosecuted counter-proliferation and economic espionage cases start out with tips provided by private industry. Three of the leading lights for the industry outreach effort are ICE-HSI's Project Shield America (PSA), the FBI's Infragard Program, and Commerce's Outreach Program. The criminal investigators who manage outreach on behalf of their agencies provide briefings to industry informing them on legal responsibilities, procedures for reporting suspicious activity red flags, and a local point of contact to which firms can provide notice after receiving questionable product inquiries. Infragard has a broader charter beyond counter-proliferation to include terrorism, critical infrastructure protection, cyber security, white collar crime, violent crime, and public corruption. Commerce's Outreach Program and ICE-HSI's PSA, by contrast, have a more specialized focus on counter-proliferation.[21]

End-Use Check Programs

Another area of concern, involves end-use check programs. For certain types of technologies and countries of heightened concern, end-use checks are a selectively useful and valuable tool for the identification of export control circumvention. The intent of end-use checks is to check and verify the *bona fides* of the recipient of restricted technology before a license is

issued, after the license is issued, and after the technology has been shipped to the recipient. Due to the large volumes of international trade flows, it is impractical to do an end use check for every licensed export. Three major programs conducting end-use checks are Department of Commerce's Sentinel, Department of State's Blue Lantern, and the Defense Security Cooperation's Agency's Golden Sentry. An essential element of all post-shipment end-use checks is physical verification of the export controlled good presence at the address stated in the EEI. End-use checks are a normal part of business for both the licensing and law enforcement communities (with some possible input from the intelligence community). End-use checks would apply to 3PLs in limited circumstances, such as when the 3PL is the consignee or a recipient of a 'collected shipment' (see Appendix B).[22]

Allied Partner Training: EXBS

Most customs services, particularly in the developing world, view their function as one of simply raising revenue as goods enter and exit their sovereign territory. The United States, and other advanced countries, have long taken a different view and see customs as a means to help make their countries, and the world at large, safer. This more broadly conceived customs enforcement effort is accomplished through the identification and interception of illicit trade flows, such as weapons, dual-use goods, narcotics, counterfeit, and stolen goods. Not all 169-member states of the World Customs Organization are at the same stage of development. The purpose of the State Department's EXBS Program, established in 2001, is to narrow this gap and help countries interested in improving how their customs services manage the enforcement of strategic trade controls. EXBS provides over a hundred different types of training and activities to address all aspects of export control licensing, criminal investigation, and counter-proliferation intelligence. Though managed by the State Department, its execution of training

activities is interagency in nature and has expertise and participation from CBP, ICE-HSI, Department of Energy, FBI, Commerce, and others. The State Department's budget request for EXBS, for FY 2019, is $59.7 million. Customs services, whether in the US or abroad, are essential to interdicting illicit trade, because it is they who often have the necessary legal authorities to both inspect cargo and seize contraband without a search warrant.[23]

Multi-Lateral Efforts: Proliferation Security Initiative and UNSCR 1540

Begun in May 2003, the Proliferation Security Initiative (PSI) is an action-oriented multi-lateral agreement that helps member nations identify and interdict WMD related illicit shipments transiting via sea, air, and land. Approximately 105 nations support PSI (notably, 88 do not). Participant states agree to share information in a timely fashion and abide by and implement a four-part list of interdiction principles. As part of the list of interdiction principles, it mentions the need to act against those involved in "transfers (either selling, receiving, or facilitating) of WMD, their delivery systems, or related materials."[24] It also asks PSI members to act if "their ports, airfields, or other facilities are used as transshipment points for shipment of such cargoes to or from states or non-state actors of proliferation concern…and to seize such cargoes that are identified."[25] PSI's Statement of Interdiction Principles does not specifically mention 3PLs by any of their various names but it does specifically mention entities selling, receiving, and facilitating transfers of WMD and WMD related materials and 3PLs can fall within this category of concern. The PSI is less an organization than it is an informal arrangement amongst signatory countries. This lack of formal organization has subjected PSI to some criticisms, including the ad-hoc nature of PSI capacity building exercises and insufficient involvement of civilian law enforcement officers. The PSI capacity building drills are most often naval ship boarding exercises.[26]

The UN Security Council passed United Nations Security Council Resolution 1540 in 2004, marking a watershed event in global counter-proliferation efforts. The resolution was passed shortly after PSI began following the December 2003 public exposure of operational details of the A.Q. Khan network. Amongst other techniques, the A.Q. Khan network used freight forwarders as consignees as well as front companies based in countries with weak export control restrictions such as United Arab Emirates, South Africa, and Turkey. A.Q. Khan illicitly smuggled dual-use nuclear technologies to Pakistan and several other prohibited end users. The most significant thing about UNSCR 1540 is it does not focus on specific nation-states (e.g. Iraq, Iran, North Korea, or Pakistan) but instead highlights the global threat of proliferation and the central role of non-state actors as proliferation agents of concern. The resolution declares it is the explicit responsibility of all the world's nation-states to regulate non-state actors who become involved in black and gray arms markets, WMD, and trade of technologies which can deliver WMD. UNSCR 1540 does not specify oversight of 3PLs by name but implicates them when declaring all nations need to have appropriate "laws and regulations to control export, transit, transshipment and re-export…that would contribute to proliferation."[27]

Future Ways Ahead: Recommended Solutions

The intent of this final section of the paper is to summarize what can be done about the 3PL issue as well as recommend possible solutions for the future, with three main avenues of approach: increased resourcing for OAIPs already in place, increased intelligence support, and a new regime of industry-specific suspicious activity reporting.

Increased Resourcing for Current OAIPs

The first recommended solution to achieve the goal of increased attention to 3PLs is continued reliance on the aforementioned OAIPs and increasing man hours and resources to the

already existing agency (FMC), as well as industry outreach and end-use verification programs. In addition, increased support to allied training and multi-lateral enforcement efforts like EXBS and the PSI. Overall, there would have to be a more explicit and pronounced focus on the 3PL industry across the board. To obtain a read on the likely success of this recommended solution, a more detailed analysis of the existing OAIPs and the metrics used by at least eight different organizations would be necessary.

Establish a National Intelligence Mission Manager Devoted to Export Control System Support

The second recommended solution, to help achieve the goal of increased attention to 3PLs, is more systematic inclusion of intelligence support throughout the overall export control process. In his 2011 essay entitled "Protecting Critical Technologies: Intelligence Support for Technology Security," Stephen Coonen advocated for the Director of National Intelligence to establish a National Intelligence Mission Manager (NIMM) office devoted to technology security and export control system support. This new NIMM office would help to ensure better situational awareness on adversary technology procurement networks, priorities, and tactics for each part of the enterprise. In Table 2, Coonen succinctly outlines the key intelligence requirements and opportunities for support.

Table 2: Intelligence Support to US Export Control

Core Area		**Intelligence Requirement/Opportunities**

What We Control	Single Control List	• Assist in Determining Tier One Technology
		• Identify Critical Foreign/Advisory Requirements
		  ○ WMD Technologies
		  ○ Dual-Use / Commercial Off-the-Shelf
		• Identify Foreign Leading-Edge Technologies
		• Assess Foreign Availability of Tier One Technology

How We Control It	Single Licensing Agency	• Integrated with Policy-Maker for Responsive Intel Support
		• Validate End-Use and End-User
		  ○ Assess End-User Capability and Intent to Protect US Technology
		  ○ Assess Diversion Risks
		• Provide Country or Technology Specific Risk Assessments
		• Leverage Transfers to Strategic Intelligence Requirements

How We Enforce Controls	Single Enforcement	• Identify Diversion of US Controlled Technologies

	Coordination Center	• Identify Attempts to Defeat of US Anti-Tamper or Protection Schemes • Monitor Rouge-State Imports • Identify and Defeat Foreign Cyber Threats to Tier One Technologies • Identify Unauthorized Transfers • Implement Technology Counter-Intelligence Program
How We Manage Our Controls	Single IT System	• Monitor Single IT System for Trends Analysis of Potential Threats, Diversions, or Unintended Consequences of US Transfers

Source: Stephen Coonen, Protecting Critical Technologies: Intelligence Support for Technology Security, 2011

There is currently an ODNI Counter-Proliferation Mission Manager, but their focus is more on what is happening inside adversary countries versus ongoing third country and US-based procurement efforts. While this course of action is broad in scope and goes well beyond the focus on 3PLs, proper resourcing and execution would help to synergize and make more effective the overall export control effort.[28]

Open Source Intelligence (OSINT) and Law Enforcement Sensitive Databases

The 16 government agencies of the Intelligence Community (IC) carry out a myriad of classified collection and analysis activities in support specific counter-proliferation efforts. However, IC collection against US persons, including US headquartered 3PLs and their management, is limited by intelligence oversight restrictions. Legal constraints on intelligence collection of US persons, while justified by civil liberties concerns, make intelligence support to the domestic side of counter-proliferation quite challenging. Consequently, an analyst's first source with which to find intelligence about US-based entities of concern, including 3PLs, is often through the collection and analysis of open source intelligence (OSINT). An additional source, of equal importance to OSINT, is the unclassified, yet law enforcement sensitive, databases of information arising from industry outreach, end-use checks, law enforcement investigations, and export records. There are multiple databases in this law enforcement

sensitive category and not all agencies have access to each other's data. This problem of multiple data streams in isolated agency-specific buckets is one of the primary reasons for the proposed four singulars (especially the single IT system).[29]

Big Data Analytics

Another tool, holding great promise for the future, is big data analytics. According to one of the leading software firms working in this area, big data analytics deals with scrutinizing "large amounts of data to uncover hidden patterns, correlations and other insights." It is about leveraging commercial off the shelf software tools, such as Hadoop, Tableau, MySQL, or Python, to take traditional statistical techniques to a higher level by quickly identifying trends and actionable information. Both DHS's Border Enforcement Analytics Program (BEAP) and the European Union's ConTraffic program are two big data analysis test beds underway and early results are promising.[30]

A New Suspicious Activity Reporting Regime Focused on 3PLs[xxvii]

The third and final recommended solution that would help achieve the goal of increased attention to 3PLs is the establishment of a 3PL industry-specific Suspicious Activity Reporting (SAR) program. The US government currently requires the banking and financial service industries to fill out and submit SARs when they come across transactions which they suspect, but do not necessarily know for certain, have a nexus to money laundering or terrorist financing. Law enforcement investigators and intelligence analysts have long relied on financial sector SARs as indicators with which to identify, analyze, and investigate potential illicit actors and

[xxvii] A June 2017 article in the *Georgetown Security Studies Review* entitled "Banking the Bomb: Improving the Engagement of Financial Institutions in Efforts to Counter Proliferation Financing," has a more detailed list of recommendations related to suspicious activity reporting and counter-proliferation finance (CPF) more broadly. The author, Darya Dolzikova, offers five specific recommendations: (1.) Developing Proliferation Specific Typologies, (2.) Improving Information Sharing Practices, (3.) Diversifying Actors Engaged in CPF Efforts: Government Agencies, (3.) Diversifying Actors Engaged in CPF Efforts: Financial Sector and Industry, and (5.) Maximizing Buy-In from Financial Institutions. A new SAR regime focused specifically on 3PLs would make a significant contribution towards improving information sharing.

networks. In principle, a similar reporting system focused on transport sector 3PLs licensed by the US government could work along similar lines. This solution would require either new legislation or amendments to the pre-existing legislation covering the SAR requirements for money laundering (the Bank Secrecy Act), terrorist financing (the PATRIOT Act), or terrorist attack indicators (DHS's National SAR Initiative [NSI]). For full implementation of this type of measure, a designated law enforcement authority would receive the 3PL SARs and conduct trend analysis, network mapping, and follow up investigations. It would also scrutinize firms not participating, as appropriate. To encourage industry cooperation, the governing legislation would need safe harbor provisions guaranteeing confidentiality and limited liability for 3PL firms submitting SARs. To further encourage industry cooperation, 3PL participation in the SAR program would be required to obtain and renew an FMC license. This reform, properly implemented, could substantially increase the transparency of the transport sector and reduce illicit trade happening via 3PLs. In addition to contributing to the fight against export control circumvention, it could also address a broader range of transnational illicit trade networks that use 3PLs to obfuscate the nature of their business. Export control reform is not just about controlling fewer, more critical items, it should also be about placing higher walls where they could be potentially helpful or necessary. A mandatory SAR reporting regime for the 3PL industry would help it to better police itself and become part of the solution. Another potentially fruitful source of suspicious activity reporting (or at least targeted industry outreach) can be found in the maritime insurance industry and customs brokers who purchase maritime insurance on behalf of clients.[31]

Concluding Thoughts

A wise man once said, "If everybody is responsible, nobody is responsible,"[32] No truer or apt words could apply more to the present state of the US export control system. Consolidation and centralization of functional responsibilities are essential to create a more efficient and effective system that balances the needs of both security and commerce. The proposed four functional singulars (one licensing agency, one control list, one IT system, and one primary enforcement coordination agency) are a long overdue set of reforms for an out of date system. However, one must remember to balance the reform of controlling fewer numbers of items at lower thresholds on one export control list with some higher walls and scrutiny where appropriate. Both control hawks and the run faster coalition should agree the 3PL industry is a logical and necessary place to start.

Appendix A: Case Summaries of 3PL Involvement in Illicit Exports[xxviii]

The illustrative case summaries below have at least one 3PL in the supply chain.

~Industrial Goods to Iran: On June 21, 2017, an indictment was unsealed charging IC Link Industries Ltd., Mohammad Khazrai Shaneivar, Arezoo Hashemnejad Alamdari, and Parisa Mohamadi, with conspiracy to export goods from the United States to Iran without the required license by the Department of the Treasury, Office of Foreign Assets Control, and to prevent officials of the US Government from detecting and preventing the export of goods from the United States to Iran. IC Link Industries Ltd. ("IC Link") registered as a corporation in Ontario, Canada, and its office was located in the Toronto area. IC Link's business included procuring industrial goods in the United States for shipment to customers in Iran. IC Link's affiliate in Tehran, Iran was Sensor Co. Ltd. ("Sensor"). Sensor was responsible for coordinating IC Link's business with Iranian companies and handling IC Link's financial dealings in Iran. According to the indictment, it was part of the conspiracy that Shaneivar, through IC Link, received orders from Alamdari and others at Sensor on behalf of customers in Iran for industrial goods available in the United States. These orders were primarily for goods used in the oil, gas, petroleum, and energy industries. IC Link sent requests for quotes ("RFQs") for the goods to an uncharged individual in Ohio, who obtained quotes from suppliers in the United States that he forwarded to IC Link. Typically, the goods were sent to the individual's business in Ohio. The goods were then shipped from the United States to an intermediary country other than Iran, such as the United Arab Emirates, Turkey, or other countries. Once the goods arrived in the intermediary country, a freight forwarder in that country reshipped the goods to Iran. While in the

[xxviii] This appendix is extracted verbatim from the cited sources, with minor omissions and edits for brevity.

intermediary country, the goods were sometimes re-packaged to disguise their origin in the United States. When shipping goods on behalf of IC Link, Mohamadi typically used a shipping company in the United States to ship the goods from Ohio to Dubai, United Arab Emirates, and other transshipment locations. Once the goods were in Dubai or elsewhere, Mohamadi used a different freight forwarding company to re-ship the goods to Iran.[33]

~Military-Grade Equipment to Ukraine: On March 7, 2017, Volodymyr Nedoviz, a citizen of Ukraine and lawful permanent resident of the United States, was arrested on federal charges of illegally exporting controlled military technology from the United States to end-users in Ukraine in violation of the Arms Export Control Act (AECA) and the International Emergency Economic Powers Act (IEEPA). Federal agents also executed a search warrant at a Philadelphia, Pennsylvania location that was used in connection with Nedoviz's illegal scheme. The complaint alleges that Nedoviz conspired with others located in both Ukraine and the United States to purchase export-controlled, military-grade equipment from sellers in the United States and to export that equipment to Ukraine without the required export licenses from the US Departments of Commerce or State. The devices obtained by the defendant and his co-conspirators included, among others, an Armasight Zeus-Pro 640 2-16x50 (60Hz) Thermal Imaging weapons sight, a FLIR Thermosight R-Series, Model RS64 60 mm 640x480 (30Hz) Rifle Scope, and an ATN X-Sight II 5-20x Smart Rifle Scope. In many cases, the devices purchased by Nedoviz and his co-conspirators retail for almost $9,000, and they are specifically marketed to military and law enforcement consumers. As part of the conspiracy, in order to induce US-based manufacturers and suppliers to sell them the export-controlled devices and to evade applicable export controls, the defendant and his co-conspirators falsely purported to be United States citizens and concealed the fact they were exporters. The defendant and his co-conspirators also recruited, trained, and paid other US-based individuals to export the controlled devices to Ukraine via various freight forwarding companies. On January 11, 2018, Nedoviz was sentenced to time served, 2 years supervised release, and forfeiture of $2,500.[34]

~Firearms Parts and Ammunition to the Philippines: On February 15, 2017, a Long Beach woman pleaded guilty to federal offenses for illegally shipping tens of thousands of rounds of ammunition to the Philippines. Marlou Mendoza, 61, pleaded guilty to three counts of failing to provide the required written notice to freight forwarders that she was shipping ammunition to a foreign country and admitted that she sent .22-caliber ammunition and bullets to the Philippines in three shipments in June 2011. The shipments contained 131,300 rounds, the defendant admitted in court. In a related case unsealed in 2016, Mark Louie Mendoza, the 31-year-old son of Marlou Mendoza, was charged with illegally shipping hundreds of thousands of dollars' worth of firearms parts and ammunition to the Philippines – munitions that were concealed in shipments falsely claimed to be household goods. Mark Mendoza, who remains a fugitive, is named in an eight-count indictment that charges him with conspiracy, the unlawful export of munitions, smuggling and money laundering. Mark Mendoza, who was the president of a tools and equipment company known as Last Resort Armaments, ordered more than $100,000 worth of ammunition and firearms accessories, much of which was delivered to his parent's Long Beach residence over a six-month period in 2011. The items that Mark MENDOZA ordered included parts for M-16 and AR-15-type rifles, and these parts are listed as defense articles on the United States Munitions List. Pursuant to the Arms Export Control Act, items on the

Munitions List may not be shipped to the Philippines without an export license issued by the Department of State.[35]

~High-Tech Electronic Components to Iran: On May 23, 2016, Ali Reza Parsa, a Canadian-Iranian dual citizen and resident of Canada, was sentenced to three years in prison for conspiracy to violate US export control laws. Between 2009 and 2015, Parsa conspired to obtain electronics from US companies for transshipment to Iran and other countries for clients of his procurement company in Iran, Tavan Payesh Mad, in violation of US economic sanctions. To accomplish this crime, Parsa used his Canadian company, Metal PM, to place orders with US suppliers and typically had the parts shipped to him in Canada or to a freight forwarder located in the United Arab Emirates. The parts where then shipped from these locations to Iran. Parsa provided the US companies with false destination and end-user information about the components to conceal the illegality of these transactions. No persons or entities involved applied for export licenses from the US Department of the Treasury's OFAC for the transactions.[36]

~Military Aviation Trade Secrets to Iran: On February 25, 2015, Mozaffar Khazaee pleaded guilty to unlawful export of defense articles from the US, in violation of the Arms Export Control Act.[xxix] Khazaee attempted to ship to Iran proprietary material relating to military jet engines and the US Air Force's F35 Joint Strike Fighter (JSF) program that he had illegally retained from defense contractors where he worked. Authorities began investigating Khazaee in November 2013, when the US Customs and Border Protection Service (CBP), assisted by HSI special agents, inspected a shipment that Khazaee sent by truck from Connecticut to a freight forwarder located in California, which was intended for shipment from the US to Iran. The documentation for Khazaee's shipment said it contained household goods. Upon inspecting the shipment, however, CBP officers and HSI special agents discovered the contents of the shipment contained numerous boxes of documents with sensitive technical manuals and other proprietary material relating to the F35 JSF program and military jet engines.[37]

~Hazardous Materials to Saudi Arabia: On February 21, 2014, Hasan Ibrahim was sentenced to 30 days' imprisonment, three years of supervised release, and a $2,200 special assessment. Previously, on July 3, 2013, Ibrahim was convicted of attempting to place destructive substances on an airplane. The jury found the subject willfully intended to place nine different hazardous materials on a Lufthansa passenger airplane bound for Frankfurt, Germany. The hazardous materials were ultimately destined for Jeddah, Saudi Arabia. In related charges, the jury convicted Ibrahim of failing to properly label the packages containing the hazardous materials and failing to complete the requisite shipping papers as required by the Department of Transportation. According to a related indictment issued in 2011, Ibrahim caused a shipment consisting of five pallets containing sixty-four boxes to be delivered to a freight forwarder for export to Saudi Arabia. None of the boxes were labeled as containing hazardous material. The shipment contained over 25 separate chemicals designated as hazardous materials under the Hazardous Materials Regulations. Two of the hazardous materials - Sulfuryl Chloride (classified as a corrosive) and Chloroacetonitrile (classified as poisonous material, with a subsidiary hazard that it is a flammable and combustible liquid) - were poisonous by inhalation and prohibited under federal law from transportation on any aircraft.[38]

[xxix] The Arms Export Control Act gives the President of the United States the authority to control the export of defense articles and defense services, including Department of Defense related proprietary information.

~Military-Grade Thermal and Night Vision Goggles to the United Kingdom and Various European Countries: On January 28, 2014, Martin Gula, a former member of the Slovakian Military Special Forces, was indicted for violations of US export control laws. Between 2006 and 2013, Gula used numerous fictitious names and an international network of suppliers, freight forwarders, mail forwarding companies, and bank accounts to illegally export US defense articles, including but not limited to military-grade thermal and night-vision goggles and scopes from the United States to the United Kingdom and various other European countries. Gula fled from authorities prior to extradition to the United States and is currently a fugitive.[39]

~Dual-Use Items to the Pakistan Atomic Energy Commission: On January 22, 2014, a federal grand jury returned an indictment against three individuals and two corporations, charging them with smuggling technology out of the United States for use by the Pakistan Atomic Energy Commission. The indictment alleged Shafqat Rana along with two conspirators in Lahore, Pakistan, used two corporations, Optima Plus International, a Pennsylvania corporation, and Afro Asian International, a Pakistani corporation, to export goods from the United States to Pakistan without first obtaining a license from the Department of Commerce. The indictment charges the defendants shipped and exported goods from the United States to restricted end-users in Pakistan while providing false and fraudulent invoices to the freight forwarders, thereby causing the freight forwarders to fail to file the required export declarations. The defendants also allegedly created false and misleading invoices given to freight forwarders which undervalued and mislabeled the goods and listed false purchasers and end-users of the goods. The items smuggled to Pakistan included infrared calibrators, thickness gauges, high temperature sensors, and air samplers. Shafqat Rana left the United States and returned to Pakistan prior to the unsealing of the indictment.[40]

~Military Night Vision Equipment to Ukraine: On May 22, 2013, Ukrainian citizen Volodomyr Ponomarenko was sentenced to 24 months in prison after pleading guilty to conspiring to violate the Arms Export Control Act by attempting to export military-grade night vision equipment from the United States to Ukraine. Ponomarenko and others purchased military-grade night vision equipment from dealers in the US and attempted to export that equipment to Ukraine without the required State Department export licenses. As part of the scheme, Ponomarenko and his co-conspirators used straw purchasers in the United States to purchase the equipment. In exchange for a fee, the straw purchasers shipped the items to various freight forwarders for export to Ponomarenko in Ukraine. The night vision scopes were intercepted prior to export by authorities who learned the subject and his co-conspirators caused the freight forwarding companies to inaccurately describe the items and to falsely state that no export license was required.[41]

~Hawk Air Defense Missile Batteries to Iran: On January 9, 2013, British businessman Christopher Tappin was sentenced to serve 33 months in prison and ordered to pay a fine of $11,357 for aiding and abetting the illegal export of defense articles in connection with his efforts to export to Iran special components of the Hawk Air Defense Missile. Tappin pleaded guilty, admitting that from December 2005 to January 2007 he aided and abetted others, including two Cyprus-based business associates, in an attempt to export zinc/silver oxide reserve batteries to Iran. These batteries, a special component of the Hawk Air Defense Missile, are on

the US Munitions List and require a license for export from the US. In October 2006, Tappin wired approximately $25,000 from a London financial institution to an account in the US as payment for five of the batteries. Using false shipping documentation, Tappin arranged for the transfer of the batteries to the United Kingdom without an export license through his specifically-designated freight forwarders in violation of export control regulations. During the investigation, Tappin agreed to reimburse the undercover agent for $5,000 in fines purportedly assessed against him by US authorities after they had seized the shipment of batteries. Tappin also caused one of his Cyprus-based business associates to travel to San Antonio in January 2007 to take delivery of the batteries, ensure that they were shipped to Tappin and to pay the undercover agent $5,000 for the fines.[42]

~Dual-Use Programmable Logic Devices to China: On December 18, 2012, federal prosecutors unsealed a 12-count indictment charging Wan Li Yuan, a resident of China, and another Chinese subject known as Jason Jiang, with export and money laundering violations for their efforts to obtain dual-use programmable logic devices (PLDs) from the United States for export to China. According to the indictment, while operating from China, Yuan and Jiang created a sophisticated scheme to conceal their true identity and location in order to mislead US companies into believing they were dealing with American customers so they could procure and send sensitive technologies to China without the required export licenses. Yuan and Jiang sought to procure PLDs made by Lattice Semiconductor Corporation in Oregon, which are designed to operate at extreme temperature ranges and which can have military applications such as in missiles and radar systems. To further his efforts, the indictment alleges that Yuan created a fake website and email addresses using the name of a legitimate New York-based company. Yuan requested US companies to ship the desired parts to the address of a freight forwarder in New York, which he also falsely represented as being associated with the New York company whose business name Yuan had stolen. Through the investigation and use of an undercover operation, investigators were able to seize approximately $414,000 in funds sent by Yuan as down payments for the PLDs.[43]

~US Missile Components to Iran: On August 27, 2010, Yi-Lan Chen, of Taiwan, was sentenced to 42 months in prison, while his Taiwan corporation, Landstar Tech Company Limited, was sentenced to one year probation. On September 9, 2011, Yi-Lan Chen was sentenced to time served, two years supervised release and a $300 special assessment. Chen was arrested in Guam on February 3, 2010 for illegally exporting dual-use commodities to Iran that have potential military applications. Customers in Iran affiliated with that nation's missile program sent orders by e-mail to Chen for specific goods. Chen then requested quotes, usually by e-mail, from US businesses and made arrangements for the sale or shipment of the goods to one of several freight forwarders in Hong Kong and Taiwan. Once in Hong Kong or Taiwan, the freight forwarders shipped the goods to Iran. In one e-mail with an Iranian customer, Chen stated, "As you know we cannot tell USA this connector is for you. So we have to tell a white lie to USA that this is for our factory in Hong Kong." Among the dual-use items that Chen shipped to Iran were 120 circular hermetic connectors and 8,500 glass-to-metal seals. While the goods have commercial applications, they also can make a significant contribution to a military or nuclear program.[44]

~Electronics to Designated Terror Entity in Paraguay: On February 19, 2010, federal authorities announced the indictment of four individuals and three Miami businesses on charges involving the illegal export of electronics to a US designated terrorist entity in Paraguay. The defendants used two freight forwarders to route consumer electronics to a business located in Paraguay that the US Treasury Department has designated as a Specially Designated Terrorist Entity on grounds that it serves as a source of fundraising for Hizballah.[45]

~Various Unlicensed Exports to Prohibited End Users in UAE, China, and Syria: From 2004 to 2006, BIS investigated and charged Federal Express (FedEx) with six export control violations. On two occasions in 2006, FedEx, caused, aided and abetted acts that facilitated the attempted unlicensed export of a PC dialogic board and electronic equipment from the United States to Mayrow in Dubai, United Arab Emirates (UAE). Mayrow was a UAE-based firm involved with the procurement of electronic components for use in IEDs against US and coalition forces. The exports to Mayrow were thwarted when delivery was halted at BIS's direction. Also, in December 2005, FedEx committed another violation when it facilitated the unlicensed export of flight simulation software to Beijing University of Aeronautics and Astronautics, an organization on the BIS Entity List. Lastly, on three occasions in 2004, FedEx facilitated the unlicensed export of printer components from the US to end users in Syria. In response to this case, Assistant Secretary for Export Enforcement David W. Mills said, "It is vital that every stakeholder in the US exporting chain remain vigilant in its efforts to prevent prohibited transactions that may be detrimental to our national security, and each will be held accountable if it fails to do so." On December 2011, FedEx agreed to pay a $370,000 civil penalty.[46]

~3PL Fails to Retain Waybill Documentation Relating to Past Shipments to Syria, Iran, and Sudan: From 2002 to 2006, DPWN Holdings (USA), Inc. (formerly known as DHL and DHL Express), unlawfully aided and abetted unlicensed exports to Syria, Iran and Sudan and failed to comply with recordkeeping requirements of the EAR and OFAC regulations. DHL failed to retain air waybills and other export control documents between 2002 and 2006 relating to thousands of shipments to Iran and Sudan. In August 6, 2009, DHL agreed to pay a civil penalty of $9,444,744 and conduct external audits covering exports to Iran, Syria and Sudan from March 2007 through December 2011.[47]

Appendix B: Red Flag Indicators of Export Control Circumvention / Diversion[xxx]

Table 3: List of Common Red Flags for Freight Forwarders		
#	**Red Flag**	**Definition**
1	Cash Payment	Use of cash is unusual for the payment of transport costs--particularly for a large or expensive transaction. The use of cash as a payment method has drastically declined in recent years, with most transport companies invoicing their customers after dispatch and using bank transfers and other forms of electronic payment.[48]
2	Payment of Freight Costs by a Third Party	It is most common that either the sender/exporter or receiver/importer pays the freight, transport or service costs for a shipment. Thus, payment by a third party—particularly a third party that does not appear to have a relationship with the sender/exporter or receiver/importer, or a third party in a country other than that of the sender/exporter or receiver/importer—may be cause for further investigation.[49]
3	Disproportionate Freight Costs	Sometimes transport costs do not appear to correspond with the nature of the goods shipped. For example, a shipment with a declared value of $50 shipped as 'priority air express' with a freight or transport cost of $350. In these cases, the disparity between the good's value and the disproportionate freight costs raises the question of why the sender/exporter is willing to pay such a high amount for a shipment with such a low value, something that could be the cause for further investigation.[50]
4	Acceptance of Standard Freight Rates	Firms usually try to negotiate freight/transport rates for their shipments. It would be unusual for a company that regularly exports to accept the standard tariff or first rate offered.[51]
5	Questionable Paperwork	Documents appearing doctored or amended in some form. For example, handwritten amendments to documentation or invoices not printed on company-branded stationery.[52]
6	Incompatible Goods	Goods shipped appear to be incompatible with a country's technical capabilities. For example, semiconductor manufacturing equipment shipped to a country that has no electronics industry. Additional verification of the customer order may be required.[53]

[xxx] This appendix is extracted verbatim from the cited source, with minor omissions and edits for brevity.

7	Dubious Descriptions	Descriptions of goods are vague or misleading. For example, items described simply as 'spare parts', 'samples', 'machine tools' or 'electrical goods'.[54]
8	Unrealistic Valuations	Declared valuations appear to be unaligned with the actual value of goods or the weight of shipments. For example, a laptop computer with a value declared as $50 or a shipment of 500 kilograms with a value declared as $100.[55]
9	Inconsistent Assessment of Shipping Size	The size of a shipment (in number of units, weight or value) appears to be inconsistent with the scale of the regular business activities of the sender/exporter or receiver/importer. For example, a customer usually orders 1 kg of ammonium nitrate and suddenly places an order for 1000 kg of the same item.[56]
10	Change of Delivery Address	Last-minute or 'after dispatch' changes to a delivery address may indicate an intention to divert a shipment to an undeclared recipient. This practice is particularly relevant when a change in delivery address involves a shipment subject to export controls. If an exported shipment was subject to controls, checks should happen with a trade compliance specialist before making any changes. If the changes to a delivery address result in a shipment transiting a different country from the original route, checks should happen to see if this change requires an export license.[57]
11	Delivery to an Unusual Address	The delivery of goods to addresses incompatible with the businesses associated with such goods may be cause for concern. For example, communication equipment delivered to a bakery or industrial-scale shipments being delivered to private addresses.[58]
12	Use of Hotels Within a Transaction	It is very difficult to verify the details of a company or individual involved in a transaction when a hotel is used as the address for delivery. Thus, hotels are often used as collection or delivery addresses in an effort to conceal the true identity of the sender/exporter or receiver/importer. Use of a hotel address by any party involved in a transaction may be cause for concern.[59]
13	Use of Transport Companies as Consignees or Receivers of Shipments	On occasion, organizations or individuals attempting to violate sanctions and controls misuse transport companies as consignees or receivers of shipments. Based on the instructions of a third party, once received, shipments may be split or re-consigned as separate transactions to parties that were unknown at the point of original dispatch.[60]
14	'Delivered in' Shipments	'Delivered in' or 'dropped off' shipments are transactions whereby the sender/exporter brings the shipment to the transport company's premises rather than have the transport company collect the shipment from the sender's/exporter's address. In some circumstances, this practice may be employed to avoid identification of the nature of the sender's/exporter's business or to hide the actual sender's/exporter's details. A form of official identification (e.g. driver's license, identification card or passport) should be checked to verify that the sender/exporter is who he or she claims to be. A copy of the document should be taken and kept on file.[61]
15	'Collected' Shipments	'Collected' or 'picked up' shipments are transactions whereby the receiver/ importer takes possession of the shipment at the transport company's premises rather than have the transport company deliver the shipment to the receiver's/importer's address. In some circumstances, this practice may be employed to avoid identification of the nature of the receiver's/importer's business or to hide the actual receiver's/importer's details. A form of official identification (e.g. a driver's license, identification card or passport) should always be checked to verify that the receiver/importer is who he or she claims to be. A copy of the document should be taken and kept on file.[62]
16	Free Trade Zones	By their very nature, free trade zones and free ports areas have simplified export, transit, trans-shipment and import procedures and processing. As such, they are prime sites for the diversion of goods to sanctioned countries and individuals. Therefore, extra diligence is required when operating in such zones.[63]
17	Employee Demands	Staff insisting on working certain shifts when a particular shipment or transaction is to be processed (particularly within high-risk areas such as warehousing, data processing, screening or loading) may indicate an internal conspiracy.[64]

18	First-Time Shippers	Although representing a new revenue stream, first-time shippers or new customers can also present a possible risk. There are numerous examples of individuals and organizations impersonating another person or company with the aim of inserting an illicit transaction into the supply chain. First time shippers or new customers should be subject to robust screening to confirm that they are in fact who they claim to be.[65]
19	Restricted Parties	If the sender/exporter or receiver/importer (or even one of those parties' employees) appears on an official restricted parties list, checks should be carried out to see if it is legally possible for the transaction to continue.[66]

Source: "Proliferation Red Flags and the Transport Sector," September 2016

Appendix C: Glossary

Table 4: Glossary	
3PLs	Third Party Logistics Providers
BEAP	Border Enforcement Analytic Program
BIS	Bureau of Industrial Security
CBP	Customs and Border Protection
CCL	Commerce Control List
CoCOM	Coordinating Committee for Multilateral Export Controls
CPF	Counter-Proliferation Finance
E2C2	Export Enforcement Coordination Center
EAR	Export Administration Regulations
EEI	Electronic Export Information
FARC	Revolutionary Armed Forces of Colombia
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FedEx	Federal Express
FinCEN	Financial Crimes Enforcement Network
FMC	Federal Maritime Commission
FPPI	Foreign Principle Party Interest
IBTL	Industrial Base Technology List
IC	Intelligence Community
ICE-HSI	Immigration and Customs Enforcement – Homeland Security Investigations

IEDs	Improvised Explosive Devices
IT	Information Technology
ITAR	International Traffic in Arms Regulations
JSF	Joint Strike Fighter
NIMM	National Intelligence Mission Manager
NSI	National SAR Initiative
NVOCCs	Non-Vessel Operating Common Carriers
OAIPs	Oversight Agencies, Initiatives, and Programs
ODNI	Office of the Director of National Intelligence
OFAC	Office of Foreign Asset Control
PSA	Project Shield America
PSI	Proliferation Security Initiative
RFQs	Requests for Quotes
SAR	Suspicious Activity Report
SECDEF	Secretary of Defense
SED	Shipper's Export Declaration
TBML	Trade Based Money Laundering
UAE	United Arab Emirates
UNSCR	United Nations Security Resolution
USML	United States Munitions List
USPPI	United States Principle Party Interest
WMD	Weapons of Mass Destruction

Notes

[1] Nate Olsen, *Making Public-Private Security Cooperation More Efficient, Effective and Sustainable*, Staff Report, (Washington, DC: The Stimson Center, December 2014), 60, https://www.stimson.org/sites/default/files/file-attachments/PIP_Staff_Report_FINAL.pdf.

[2] Andrew Kuzrok, and Gretchen Hund, "Stopping Illicit Procurement: Lessons from Global Finance," *Arms Control Today*, (Washington DC: Arms Control Association, June 2, 2014), https://www.armscontrol.org/act/2014_06/Features/Stopping-Illicit-Procurement-Lessons-From-Global-Finance.

[3] Act of December 22, 1807, ch. 5, 2 Stat. 451 (1807) (amended by Act of January 9, 1808, ch. 8, 2 Stat. 453 (1808), and Act of March 12, 1808, ch. 33, 2 Stat. 473 (1808)) ("An act laying an embargo on all ships and vessels in the ports and harbors of the United States"); Non-Intercourse Act of 1809, ch. 24, 2 Stat. 528 ("An Act to interdict the commercial intercourse between the United States and Great Britain and France, and their dependencies; and for other purposes"); Embargo Act of 1813, ch. 1, 3 Stat. 88 ("An Act laying an embargo on all ships and vessels in the ports and harbors of the United States"); Reginald Horsman, *The Causes of the War of 1812* (Philadelphia, PA: University of Pennsylvania Press, 1962), 123-143; Trading with the Enemy Act, 12 U.S.C. §§ 95a–95b and 50 U.S.C. App. §§ 1–44 (1917), https://www..treasury.gov/resource-center/sanctions/Documents/twea.pdf.; John Walters, "The Official Bulletin of the United States: America's First Official Gazette." *Government Publications Review,* 19 (May-June 1992): 243-256; Bert Chapman, "Revenue, US Government," in *The Encyclopedia of the Wars of the Early American Republic, 1783-1812: A*

Political, Social, and Military History, ed. Spencer C. Tucker (Santa Barbara, CA: ABC-CLIO, 2014), 2:573-574.

[4] Noemi Mintal, "Export control of dual-use items during the cold war and in Hungary today," *Academic Applied Research in Military and Public Management Science (AARMS)* Vol 7, no. 3 (2008): 398, http://www.zmne.hu/aarms/docs/Volume7/Issue3/pdf/01mint.pdf.

[5] Stefan T. Possony, and Jerry E. Pournelle, *The Strategy of Technology: Winning the Decisive War* (Cambridge, MA: University Press of Cambridge, Inc., 1970), ix; US Congress. Office of Technology Assessment, *Technology and East-West Trade* (Washington DC: Government Printing Office, 1979), 153-170, https://www.princeton.edu/~ota/disk3/1979/7918/791810.PDF.

[6] Robert Gates, "Business Executives for National Security (Export Control Reform)," (speech, Washington DC, April 20, 2010), US Department of Defense, http://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1453.

[7] Chris Tafe, *Export Control Reform Initiative* (Homeland Security Investigations Counter-Proliferation Investigations Training Seminar, Glynco, GA, June 15-19, 2015) PowerPoint presentation.

[8] Export Compliance Solutions, "Export Control Reform Moving Along: A Report from DTAG," accessed December 28, 2017, http://exportcompliancesolutions.com/blog/2017/09/28/export-control-reform-moving-along-report-dtag/; The White House, Executive Order 13558, 75 FR 69573-69574, Export Coordination Enforcement Center, November 9, 2010, https://www.gpo.gov/fdsys/pkg/FR-2010-11-15/pdf/2010-28854.pdf; Export.gov, "5-Export Control Reform," *Export.gov*, accessed December 22, 2017, https://www.export.gov/article?id=Export-Control-Reform-ECR; 2016.Export.gov, "Export Enforcement Coordination Center (E2C2)," *2016.Export.gov*, accessed December 22, 2017, https://2016.export.gov/e2c2/; "The Path Forward on Export Control Reform," YouTube video, February 4, 2017, 1:29:39, https://www.youtube.com/watch?v=OLExhgSiK7A.

[9] Stuart Macdonald, *Technology and the Tyranny of Export Controls: Whisper Who Dares* (London: Macmillan Press Ltd, 1990), 72.

[10] Hugo Meijer, *Trading With the Enemy: The Making of US Export Control Policy Toward the People's Republic of China* (New York: Oxford University Press, 2016), 146.

[11] Aaron Dunne, *The Role of Transit and Trans-Shipment in Counterproliferation Efforts*, Stockholm International Peace Research Institute Good Practice Guide, The Transport Sector as Counterproliferation Partner (Stockholm, Sweden: Stockholm International Research Institute, September 2016), 1, https://www.sipri.org/sites/default/files/SIPRIGPG%20Transport%2006_Dunne.pdf; John Manners-Bell, and Ken Lyon, The Future of Logistics: What Does the Future Hold for Freight Forwarders?, Kewill Transport Intelligence (Manchester, UK: Blujay Solutions, September 2015),3-5, http://406wgw3346mpao4bj1jjj3q1.wpengine.netdna-cdn.com/wp-content/uploads/2015/10/Ti_The_Future_of_Logistics_Kewill_2015.pdf; Brad Dechter, "3PL or Freight Forwarder: What's in a Name?," *InboundLogistics.com*, last modified June 15, 2008, http://www.inboundlogistics.com/cms/article/3pl-or-freight-forwarder-whats-in-a-name/.

[12] Nikos Passas, and Kimberly Jones, "The Regulation of Non-Vessel-Operating Common Carriers (NVOCC) and Customs Brokers: Loopholes Big Enough to Fit Container Ships," *Journal of Financial Crime* 14, no. 1 (January 2007): 84.

[13] Lisa Fu, "US Exports Increased in June but so Did the US-China Trade Deficit," *Fortune*, August 4, 2017, http://fortune.com/2017/08/04/trade-deficit-export/; Nate Olsen, *Making Public-Private Security Cooperation More Efficient, Effective and Sustainable*, Staff Report,

(Washington, DC: The Stimson Center, December 2014), 53, https://www.stimson.org/sites/default/files/file-attachments/PIP_Staff_Report_FINAL.pdf.
[14] Department of Justice, *Summary of Major US Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases: January 2014 to the present: updated February 17, 2017* (Washington DC: Department of Justice, 2017), 1-54, https://www.justice.gov/nsd/page/file/940591/download; Department of Commerce, Bureau of Industrial Security, *Don't Let This Happen to You!!!: Actual Investigations of Export Control and Antiboycott Violations*, 56-57, https://www.sipri.org/sites/default/files/United-States-1-BIS-Dont-let-this-happen-to-you--21366_doc_web_pdf---Copy.pdf.
[15] Jamie Joiner, and Ashley Moore, "Compliance for Exporters and Freight Forwarders: A Shared Approach," in *The Export Compliance Manager's Handbook*, ed. Tom Blass (London, UK: D.C. Houghton Ltd., 2017), 198-199; Bureau of Industry and Security, US Department of Commerce. Red Flag Indicators: Things to Look for in Export Transactions. Washington DC: Department of Commerce, 2017. https://www.bis.doc.gov/index.php/enforcement/oee/compliance/23-compliance-a-training/51-red-flag-indicators; Martin Palmer, *Proliferation Red Flags and the Transport Sector*, Stockholm International Peace Research Institute Good Practice Guide, The Transport Sector as Counterproliferation Partner (Stockholm, Sweden: Stockholm International Research Institute, September 2016), 2-5, https://www.sipri.org/sites/default/files/SIPRIGPG%20Transport%2003_Palmer.pdf.
[16] "Routed Exports: Dangers For Freight Forwarders," YouTube video, Nov 22, 2016, 4:18, https://www.youtube.com/watch?v=DhtOHgKIXeE; Jamie Joiner, and Ashley Moore, "Compliance for Exporters and Freight Forwarders: A Shared Approach," in *The Export Compliance Manager's Handbook*, ed. Tom Blass (London, UK: D.C. Houghton Ltd., 2017), 201-202; "Routed Exports: Dangers to the Exporter and USPPIs," YouTube video, Dec 27, 2016, 6:03, https://www.youtube.com/watch?v=FOJdd22YSVk.
[17] Nikos Passas, and Kimberly Jones, "The Regulation of Non-Vessel-Operating Common Carriers (NVOCC) and Customs Brokers: Loopholes Big Enough to Fit Container Ships," *Journal of Financial Crime* 14, no. 1 (January 2007): 85-86.
[18] Douglas Farah, and Stephen Braun, *Merchant of Death: Money, Guns, Planes, and the Man Who Makes War Possible* (Hoboken, NJ: John Wiley & Sons, Inc., 2007), 27-28.
[19] Department of Justice, *International Arms Dealer Viktor Bout Convicted in New York of Terrorism Crimes* (Washington DC: Department of Justice, 2011), https://www.justice.gov/opa/pr/international-arms-dealer-viktor-bout-convicted-new-york-terrorism-crimes.
[20] Interview with two senior government employees, July 17, 2017.
[21] US Immigration and Customs Enforcement, *Project Shield America*, accessed 9 January 2018, https://www.ice.gov/project-shield-america; Federal Bureau of Investigation, *Infragard*, accessed 9 January 2018, https://www.infragard.org/; Department of Commerce, Bureau of Industrial Security, *Outreach Program*, accessed 9 January 2018, https://www.bis.doc.gov/index.php/2015-10-29-20-18-41/2015-10-27-14-54-3.
[22] Department of Commerce, Bureau of Industrial Security, *Sentinel*, accessed 9 January 2018, https://www.bis.doc.gov/index.php/2015-10-29-20-18-41/2015-10-27-14-54-3; Department of State, *Blue Lantern End Use Monitoring Program*, accessed 9 January 2018, https://www.pmddtc.state.gov/documents/slides/Blue%20Lantern%20End-Use%20Monitoring%20Program.pdf; Defense Security Cooperation Agency, End Use

Monitoring (EUM) Division, accessed 9 January 2018, http://www.dsca.mil/about-us/end-use-monitoring-eum; Martin Palmer, *Proliferation Red Flags and the Transport Sector*, Stockholm International Peace Research Institute Good Practice Guide, The Transport Sector as Counterproliferation Partner (Stockholm, Sweden: Stockholm International Research Institute, September 2016), 4-5, https://www.sipri.org/sites/default/files/SIPRIGPG%20Transport%2003_Palmer.pdf.

[23] Department of State, *The EXBS Program*, accessed 9 January 2018, https://www.state.gov/strategictrade/program/index.htm; David Widdowson, "The Changing Role of Customs: Evolution or Revolution," *World Customs Journal*, Volume 1, No. 1 (2007): 31-37, http://worldcustomsjournal.org/Archives/Volume%201,%20Number%201%20(Mar%202202)/00%20Complete%20Issue%20WCJ_Volume_1_Number_1.pdf#page=39; Department of State, Foreign Operations and Related Programs, *Congressional Budget Justification: Fiscal Year 2019* (Washington DC, Department of State, 2018), 113, https://www.state.gov/documents/organization/277155.pdf.

[24] Department of State, "Statement of Interdiction Principles," Under Secretary for Arms Control and International Security, Bureau of International Security and Nonproliferation (ISN), Proliferation Security Initiative, accessed January 11, 2018, https://www.state.gov/t/isn/c27726.html.

[25] *Ibid.*

[26] Mark Esper, and Susan Koch, The Proliferation Security Initiative: A Model for Future International Collaboration, (Fairfax, VA: National Institute Press, 2009), 35, http://www.nipp.org/wp-content/uploads/2014/12/The-Proliferation-Security-Initiative-txt.pdf; Jacek Durkalec, *The Proliferation Security Initiative: Evolution and Future Prospects*, Stockholm International Peace Research Institute Non-Proliferation Paper No. 16, (Stockholm, Sweden: Stockholm International Research Institute, June 2012), 1, https://www.sipri.org/sites/default/files/EUNPC_no-16.pdf.

[27] Peter Van Ham and Olivia Bosch, Global Non-Proliferation and Counter-Terrorism: The Impact of UNSCR 1540 (Baltimore, MD: Brookings Institution Press, 2007), 4; International Institute for Strategic Studies, *Nuclear Black Markets: Pakistan, A.Q. Khan and the Rise of Proliferation Networks: A Net Assessment*, (London, UK: The International Institute for Strategic Studies, 2007), 150-156.

[28] *Ibid.*

[29] Daniel M. Green, "Monitoring Technology Proliferation: An Open Source Methodology for Generating Proliferation Intelligence," (master's thesis, Naval Postgraduate School, 1993), 45-67.

[30] SAS.com, "Big Data Analytics: What it is and Why it Matters," *SAS.com*, accessed January 13, 2018, https://www.sas.com/en_us/insights/analytics/big-data-analytics.html; Department of Homeland Security (DHS), "Border Enforcement Analytics Program Apex Infographic," *dhs.gov*, accessed January 13, 2018, https://www.dhs.gov/science-and-technology/beap-apex-infographic; European Commission, "Container Traffic Monitoring System," *EU Science Hub*, accessed January 13, 2018, https://ec.europa.eu/jrc/en/scientific-tool/container-traffic-monitoring-system.

[31] Andrew Kuzrok, and Gretchen Hund, "Stopping Illicit Procurement: Lessons from Global Finance," *Arms Control Today*, (Washington DC: Arms Control Association, June 2, 2014), https://www.armscontrol.org/act/2014_06/Features/Stopping-Illicit-Procurement-Lessons-From-

Global-Finance; G Hund, et al., "Meeting Summary of Kitchen Cabinet on Financial Due Diligence to Reduce Proliferation Risks," *Pacific Northwest National Laboratory (PNNL-25676),* (Richland, WA: US Department of Energy, July 2016), 5, https://cgs.pnnl.gov/pdfs/Kitchen_Cabinet_Abbrev8-10-16.pdf.; Darya Dolzikova, "Banking the Bomb: Improving the Engagement of Financial Institutions in Efforts to Counter Proliferation Financing," *Georgetown Security Studies Review* 5, Issue 2 (June 2017): 54-62, http://georgetownsecuritystudiesreview.org/wp-content/uploads/2017/06/GSSR-5.2-June-2017.pdf.

[32] Roy Snell, "If Everybody is Responsible, Nobody is Responsible," *Society of Corporate Compliance and Ethics (SCCE),* last modified March 12, 2015, http://complianceandethics.org/if-everybody-is-responsible-nobody-is-responsible/.

[33] Department of Justice, *Summary of Major US Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases: January 2015 to the present: updated January 19, 2018* (Washington DC: Department of Justice, 2018), 6, https://www.justice.gov/nsd/page/file/1044446/download.

[34] Department of Justice, *Summary of Major US Export Enforcement Cases 2018,* 11.

[35] Department of Justice, *Summary of Major US Export Enforcement, Cases 2018,* 14.

[36] Department of Justice, *Summary of Major US Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases: January 2014 to the present: updated February 17, 2017* (Washington DC: Department of Justice, 2017), 19, https://www.justice.gov/nsd/page/file/940591/download.

[37] Department of Justice, *Summary of Major US Export Enforcement Cases 2017*, 24-25.

[38] Department of Justice, *Summary of Major US Export Enforcement Cases 2017*, 51-52.

[39] Department of Justice, *Summary of Major US Export Enforcement Cases 2017*, 52.

[40] Department of Justice, *Summary of Major US Export Enforcement Cases 2017*, 52-53.

[41] Department of Justice, *Summary of Major US Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases: January 2008 to the present: updated January 23, 2015* (Washington DC: Department of Justice, 2015), 32.

[42] Department of Justice, *Summary of Major US Export Enforcement Cases 2015*, 37-38.

[43] Department of Justice, *Summary of Major US Export Enforcement Cases 2015*, 38.

[44] Department of Justice, *Summary of Major US Export Enforcement Cases 2015*, 72-73.

[45] Department of Justice, *Summary of Major US Export Enforcement Cases 2015*, 72-75.

[46] Department of Commerce, Bureau of Industrial Security, *Don't Let This Happen to You!!!: Actual Investigations of Export Control and Antiboycott Violations*, 56, https://www.sipri.org/sites/default/files/United-States-1-BIS-Dont-let-this-happen-to-you--21366_doc_web_pdf---Copy.pdf.

[47] Department of Commerce, Bureau of Industrial Security, *Don't Let This Happen to You!!!: Actual Investigations of Export Control and Antiboycott Violations*, 57.

[48] Martin Palmer, *Proliferation Red Flags and the Transport Sector,* Stockholm International Peace Research Institute Good Practice Guide, The Transport Sector as Counterproliferation Partner (Stockholm, Sweden: Stockholm International Research Institute, September 2016), 2, https://www.sipri.org/sites/default/files/SIPRIGPG%20Transport%2003_Palmer.pdf.

[49] Martin Palmer, *Proliferation Red Flags and the Transport Sector,* 2.

[50] Martin Palmer, *Proliferation Red Flags and the Transport Sector,* 2.

[51] Martin Palmer, *Proliferation Red Flags and the Transport Sector,* 2.

[52] Martin Palmer, *Proliferation Red Flags and the Transport Sector,* 3.

[53] Martin Palmer, *Proliferation Red Flags and the Transport Sector*, 3.
[54] Martin Palmer, *Proliferation Red Flags and the Transport Sector*, 3.
[55] Martin Palmer, *Proliferation Red Flags and the Transport Sector*, 3.
[56] Martin Palmer, *Proliferation Red Flags and the Transport Sector*, 3.
[57] Martin Palmer, *Proliferation Red Flags and the Transport Sector*, 3.
[58] Martin Palmer, *Proliferation Red Flags and the Transport Sector*, 4.
[59] Martin Palmer, *Proliferation Red Flags and the Transport Sector*, 4.
[60] Martin Palmer, *Proliferation Red Flags and the Transport Sector*, 4.
[61] Martin Palmer, *Proliferation Red Flags and the Transport Sector*, 4.
[62] Martin Palmer, *Proliferation Red Flags and the Transport Sector*, 5.
[63] Martin Palmer, *Proliferation Red Flags and the Transport Sector*, 5.
[64] Martin Palmer, *Proliferation Red Flags and the Transport Sector*, 5.
[65] Martin Palmer, *Proliferation Red Flags and the Transport Sector*, 5.
[66] Martin Palmer, *Proliferation Red Flags and the Transport Sector*, 5.

Bibliography

Argue, William. *HSI Authorities.* PowerPoint presentation. Homeland Security Investigations Counter-Proliferation Investigations Training Seminar, Glynco, GA, June 15-19, 2015.

Bryen, Stephen D. *Technology Security and National Power: Winners and Losers*. New Brunswick, NJ: Transaction Publishers, 2016.

Chapman, Bert. *Export Controls: A Contemporary History*. Lanham, MD: University Press of America, 2013.

Chapman, Bert. "Revenue, US Government." In *The Encyclopedia of the Wars of the Early American Republic, 1783-1812: A Political, Social, and Military History*. Edited by Spencer C. Tucker, 2:573-574. Santa Barbara, CA: ABC-CLIO, 2014.

Coonen, Steven. *Protecting Critical Technologies: Intelligence Support for Technology Security*. Washington DC: Armed Forces Communications and Electronics Association, 2011. https://www.afcea.org/content/protecting-critical-technologies-intelligence-support-technology-security.

Cuppitt, Richard T. *Reluctant Champions: US Presidential Policy and Strategic Export Controls*. New York: Routledge, 2000.

Department of Commerce, Bureau of Industry and Security. US Department of Commerce. *Red Flag Indicators: Things to Look for in Export Transactions*. Washington DC: Department of Commerce, 2017.

https://www.bis.doc.gov/index.php/enforcement/oee/compliance/23-compliance-a-training/51-red-flag-indicators.

Department of Commerce, Bureau of Industry and Security. *Annual Report to the Congress for Fiscal Year 2016*. Washington DC: Department of Commerce, 2016. https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/1629-bis-report-to-congress-fy-2016/file.

Department of Commerce, Bureau of Industry and Security. *Don't Let This Happen to You!!!: Actual Investigations of Export Control and Antiboycott Violations*. https://www.sipri.org/sites/default/files/United-States-1-BIS-Dont-let-this-happen-to-you--21366_doc_web_pdf---Copy.pdf.

Department of Defense, Defense Security Service. *Counterintelligence Awareness Job Aid Series: Industrial Base Technology List.* https://www.cdse.edu/documents/cdse/CI-JobAidSeries-IBTL.pdf

Department of Justice. *Summary of Major US Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases: January 2015 to the present: updated January 19, 2018*. Washington DC: Department of Justice, 2018. https://www.justice.gov/nsd/page/file/1044446/download.

Department of Justice. *Summary of Major US Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases: January 2014 to the present: updated February 17, 2017*. Washington DC: Department of Justice, 2017. https://www.justice.gov/nsd/page/file/940591/download.

Department of Justice. *Summary of Major US Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases: January 2008 to the present: updated January 23, 2015*. Washington DC: Department of Justice, 2015.

Department of Justice. *International Arms Dealer Viktor Bout Convicted in New York of Terrorism Crimes*. Washington, DC: Department of Justice, 2011. https://www.justice.gov/opa/pr/international-arms-dealer-viktor-bout-convicted-new-york-terrorism-crimes.

Department of State. "Statement of Interdiction Principles." Under Secretary for Arms Control and International Security, Bureau of International Security and Nonproliferation (ISN), Proliferation Security Initiative. https://www.state.gov/t/isn/c27726.html.

Department of State, Foreign Operations and Related Programs, *Congressional Budget Justification: Fiscal Year 2019* (Washington DC, Department of State, 2018), 113. https://www.state.gov/documents/organization/277155.pdf.

Dolzikova, Darya, "Banking the Bomb: Improving the Engagement of Financial Institutions in

Efforts to Counter Proliferation Financing." *Georgetown Security Studies Review* 5, Issue 2 (June 2017): 54-62. http://georgetownsecuritystudiesreview.org/wp-content/uploads/2017/06/GSSR-5.2-June-2017.pdf.

Dunne, Aaron. *The Role of Transit and Trans-Shipment in Counterproliferation Efforts*. Stockholm International Peace Research Institute Good Practice Guide, The Transport Sector as Partner. Stockholm, Sweden: Stockholm International Research Institute, September 2016. https://www.sipri.org/sites/default/files/SIPRIGPG%20Transport%2006_Dunne.pdf.

Durkalec, Jacek. *The Proliferation Security Initiative: Evolution and Future Prospects*. Stockholm International Peace Research Institute Non-Proliferation Paper No. 16. Stockholm, Sweden: Stockholm International Research Institute, June 2012. https://www.sipri.org/sites/default/files/EUNPC_no-16.pdf.

Esper, Mark, and Susan Koch. *The Proliferation Security Initiative: A Model for Future International Collaboration*. Fairfax, VA: National Institute Press, 2009. http://www.nipp.org/wp-content/uploads/2014/12/The-Proliferation-Security-Initiative-txt.pdf.

Farah, Douglas, and Stephen Braun. *Merchant of Death: Money, Guns, Planes, and the Man Who Makes War Possible*. Hoboken, NJ: John Wiley & Sons, Inc., 2007.

Federal Maritime Commission, Ocean Transportation Intermediaries (OTI) List. Washington DC: Federal Maritime Commission, 2018. https://www2.fmc.gov/oti/NVOCC.aspx.

Fitzgerald, David R. "Leaving the Back Door Open: How Export Control Reform's Deregulation May Harm America's Security." North Carolina Journal of Law & Technology 15 N.C. J.L. & Tech On. 65 (2014): 65-99.

Fu, Lisa. "US Exports Increased in June but so Did the US-China Trade Deficit." *Fortune*, August 4, 2017. http://fortune.com/2017/08/04/trade-deficit-export/.

Gates, Robert. "Business Executives for National Security: Export Control Reform." Speech. Washington DC, April 20, 2010, US Department of Defense. http://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1453.

Green, Daniel M. "Monitoring Technology Proliferation: An Open Source Methodology for Generating Proliferation Intelligence." Master's thesis. Naval Postgraduate School, 1993.

Horsman, Reginald. *The Causes of the War of 1812*. Philadelphia, PA: University of Pennsylvania Press, 1962.

Hund, G., et al. "Meeting Summary of Kitchen Cabinet on Financial Due Diligence to Reduce

Proliferation Risks," *Pacific Northwest National Laboratory (PNNL-25676)*. Richland, WA: US Department of Energy, July 2016. https://cgs.pnnl.gov/pdfs/Kitchen_Cabinet_Abbrev8-10-16.pdf.

International Institute for Strategic Studies. *Nuclear Black Markets: Pakistan, A.Q. Khan and the Rise of Proliferation Networks: A Net Assessment*. London, UK: The International Institute for Strategic Studies, 2007.

Joiner, Jamie, and Ashley Moore. "Compliance for Exporters and Freight Forwarders: A Shared Approach." In *The Export Compliance Manager's Handbook*, edited by Tom Blass, 198-199. London, UK: D.C. Houghton Ltd., 2017.

Kuzrok, Andrew, and Gretchen Hund. "Stopping Illicit Procurement: Lessons From Global Finance." *Arms Control Today*. June 2, 2014, https://www.armscontrol.org/act/2014_06/Features/Stopping-Illicit-Procurement-Lessons-From-Global-Finance.

Macdonald, Stuart. *Technology and the Tyranny of Export Controls: Whisper Who Dares*. London: Macmillan Press Ltd, 1990.

Manners-Bell, John, and Ken Lyon. *The Future of Logistics: What Does the Future Hold for Freight Forwarders?* Kewill Transport Intelligence. Manchester, UK: Blujay Solutions, September 2015. http://406wgw3346mpao4bj1jjj3q1.wpengine.netdna-cdn.com/wp-content/uploads/2015/10/Ti_The_Future_of_Logistics_Kewill_2015.pdf.

Meijer, Hugo. *Trading With the Enemy: The Making of US Export Control Policy Toward the People's Republic of China.* New York: Oxford University Press, 2016.

Metcalfe, Robyn Shotwell. *The New Wizard War: How the Soviets Steal US High Technology—And How We Give It Away.* Redmond, WA: Tempus Books of Microsoft Press, 1988.

Mintal, Noemi. "Export control of dual-use items during the cold war and in Hungary today." *AARMS* Vol 7, 3 (2008): http://www.zmne.hu/aarms/docs/Volume7/Issue3/pdf/01mint.pdf.

National Academies Press. *Export Control Challenges Associated With Securing the Homeland*. Washington DC: National Research Council of the National Academies, Committee on Homeland Security and Export Controls, 2012.

National Academies Press. *Beyond 'Fortress America': National Security Controls on Science and Technology in a Globalized World*. Washington DC: National Research Council of the National Academies; Policy and Global Affairs; Development, Security; and Cooperation, Committee on Science, Security, and Prosperity; Committee on Scientific Communication and National Security, 2009.

Olsen, Nate. *Making Public-Private Security Cooperation More Efficient, Effective and*

Sustainable. Washington, DC: The Stimson Center, December 2014. https://www.stimson.org/sites/default/files/file-attachments/PIP_Staff_Report_FINAL.

Palmer, Martin. *Proliferation Red Flags and the Transport Sector*. Stockholm International Peace Research Institute Good Practice Guide, the Transport Sector as Counterproliferation Partner. Stockholm, Sweden: Stockholm International Research Institute, September 2016. https://www.sipri.org/sites/default/files/SIPRIGPG%20Transport%2003_Palmer.pdf.

Pasco, Brandt. "The Case for Export Control Reform, and What it Means for America." *Harvard Law School National Security Journal* (October 19, 2014): http://harvardnsj.org/2014/10/the-case-for-export-control-reform-and-what-it-means-for-america/.

Passas, Nikos, and Kimberly Jones. "The Regulation of Non-Vessel-Operating Common Carriers (NVOCC) and Customs Brokers: Loopholes Big Enough to Fit Container Ships." *Journal of Financial Crime* 14, no. 1 (January 2007).

Possony, Stefan T., and Jerry E. Pournelle. *The Strategy of Technology: Winning the Decisive War*. Cambridge, MA: University Press of Cambridge, Inc., 1970.

Snell, Roy. "If Everybody is Responsible, Nobody is Responsible." *Society of Corporate Compliance and Ethics (SCCE),* last modified March 12, 2015, http://complianceandethics.org/if-everybody-is-responsible-nobody-is-responsible/.

Stricker, Andrea, and David Albright. *US Export Control Reform: Impacts and Implications for Controlling the Export of Proliferation-Sensitive Goods and Technologies.* Washington DC: Institute for Science and International Security, May 17, 2017. http://isis-online.org/isis-reports/detail/u.s.-export-control-reform-impacts-and-implications.

Tafe, Chris. *Export Control Reform Initiative.* PowerPoint Presentation. Homeland Security Investigations Counter-Proliferation Investigations Training Seminar, Glynco, GA, June 15-19, 2015.

US Congress. Office of Technology Assessment, *Technology and East-West Trade* (Washington DC: Government Printing Office, 1979), https://www.princeton.edu/~ota/disk3/1979/7918/791810.PDF.

Walters, John. "The Official Bulletin of the United States: America's First Official Gazette." *Government Publications Review*, 19 (May-June 1992): 243-256.

The White House, Executive Order 13558. Export Coordination Enforcement Center. November 9, 2010. https://obamawhitehouse.archives.gov/the-press-office/2010/11/09/executive-order-13558-export-coordination-enforcement-center.

Van Ham, Peter, and Olivia Bosch. *Global Non-Proliferation and Counter-Terrorism: The Impact of UNSCR 1540*. Baltimore, MD: Brookings Institution Press, 2007.

Widdowson, David. "The Changing Role of Customs: Evolution or Revolution." *World Customs Journal* Volume 1, No. 1 (2007). http://worldcustomsjournal.org/Archives/Volume%201,%20Number%201%20(Mar%202202)/00%20Complete%20Issue%20WCJ_Volume_1_Number_1.pdf#page=39.