Export Control Laws

In This Issue

November 2013
Volume 61
Number 6

United States
Department of Justice
Executive Office for
United States Attorneys
Washington, DC
20530

H. Marshall Jarrett
Director

The United States Attorneys' Bulletin is published pursuant to 28 CFR § 0.22(b).

The United States Attorneys' Bulletin is published bimonthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201.

Managing Editor
Jim Donovan

Legal Assistant
Carmel Matin

Law Clerk
Jennifer Jokerst

Internet Address
www.usdoj.gov/usao/reading_room/foiamanuals.html

Send article submissions and address changes to Managing Editor, United States Attorneys' Bulletin, National Advocacy Center, Office of Legal Education, 1620 Pendleton Street, Columbia, SC 29201.

Extradition in Export Enforcement Cases

Ryan P. Fayhee
Acting Deputy Chief
National Export Enforcement Coordinator
Counterespionage Section
National Security Division

I. Introduction

Efforts by the Department of Justice and our partners in the law enforcement and intelligence communities are making it substantially more difficult for proliferators to obtain restricted technology and services from the United States. The seizure of just one piece of restricted technology, however innocuous it may seem, can have a tremendous impact on a foreign adversary's capabilities. The investigation and prosecution of such conduct is well worth our time, energy, and resources.

In recent years, the prosecution of individuals and companies, wherever located, who exploit the U.S. market by stealing sensitive technology or who procure goods from the United States on behalf of designated organizations has resulted in positive developments all across the globe. As a result of the threat of proliferation, many foreign partners have enacted more severe export controls and financial restrictions or, in some instances, created controls that did not previously exist. For instance, the European Union (E.U.) has developed export controls in much the same way as the United States, evolving as necessary to stem an increasingly dynamic threat. Even global transshipment states with economies that rely on speedy and unencumbered trade, such as Malaysia and the United Arab Emirates, have enacted domestic export controls with serious criminal penalties.

Ongoing law enforcement cooperation, foreign prosecutor training, and other capacity-building efforts are of great benefit to our counter-proliferation mission and have resulted in successful extraditions from countries around the world, including, but not limited to, Bulgaria, Canada, the Czech Republic, Estonia, Georgia, Germany, Hong Kong, Hungary, Singapore, and the United Kingdom. The commodities at issue, some with both military and commercial application, have been as varied as the countries themselves and include vacuum pumps, thermal imaging cameras, accelerometers, radiation-hardened electronics, Hawk missile components, and circuit boards recovered from improvised explosive devices in Iraq.

As set out further below, recent successful extraditions are also the product of charging and conveying the violations in a way that accurately depicts the deceptive nature of the crime as well as its seriousness. At the very least, when crafted carefully, the extradition process tends to be considered by our treaty partners in a more timely and efficient manner.

II. Foreign actors and middlemen

U.S. export control statutes are not extraterritorial but rather apply to goods and services exported from the United States and to the conduct of U.S. persons (that is, U.S. citizens, legal permanent resident aliens, and persons present in the United States). In many instances, foreign procurement agents and middlemen have availed themselves of U.S. jurisdiction by contacting U.S. companies and misrepresenting the purpose and nature of their purchases, wiring money into the United States under false pretenses, and filing fraudulent shipping records with export control agencies. In the context of dual-

use commodities, U.S. companies are often told that the technology in question is destined for a third country and will remain there for valid uses. Based on these false representations, the U.S. manufacturer will export the goods to an intermediate country before they are ultimately diverted to a prohibited end-user.

Within the export community, shippers are often responsible for completing the shipping paperwork, which includes documents that accompany the export, such as air waybills and documents filed with government agencies, such as Shippers Export Declarations. U.S. prosecutors have charged and continue to charge individuals who provide false information to their U.S shippers because they are perpetrating a fraud by causing a false statement to be made to the U.S. Government. False information contained in these shipping documents can be used to avoid detection by systems that help the Government to detain illicit exports at the border.

The Internet has clearly played an enormous role in these transactions. Proliferators spearheading these procurement networks are able to quickly locate products for sale anywhere in the world with just a few keystrokes. They are then able to communicate that information via email to their middlemen overseas and direct them to specific U.S. suppliers. These foreign middlemen agents may change their names frequently and may never see or touch the products they order from the United States. They 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. The location of the middlemen may or may not be in the same country as the shipping route of the goods or the flow of money. For example, a trading company in the Netherlands may order goods from the United States but cause them to be shipped to Malaysia, where they are then sent to Iran. The money may flow along an entirely different route. Taking these extra steps results in transactional costs that are much higher, but so too are the opportunities for these illicit firms to take advantage of their customers, allowing the middlemen to profit considerably.

III. Establishing dual criminality

Many modern extradition treaties provide for extradition where the conduct charged is punishable under the law of both the requesting and requested states, regardless of whether both states punish those acts as precisely the same type of offense or category of offenses or whether the offense is described by the same terminology. The essential consideration is whether the nature of the conduct is criminalized in both states, rather than the manner in which the offenses are denominated. In that regard, U.S. courts have ruled in favor of extradition even where the offense charged in the foreign country seeking extradition was quite different from that which would be applied had the conduct taken place in the United States. The Supreme Court interpreted dual criminality concisely nearly a century ago:

> The law does not require that the name by which the crime is described in the two countries shall be the same; nor that the scope of the liability shall be coextensive, or, in other respects, the same in the two countries. It is enough if the particular act charged is criminal in both jurisdictions.

Collins v. Loisel, 259 U.S. 309, 312 (1922). *See also Matter of Extradition of Matus*, 784 F. Supp. 1052, 1055 (S.D.N.Y. 1992) (ruling in favor of extradition to Chile of an offender who evaded Chile's value added tax, where the conduct could have been punishable under different U.S. offenses, including, for example, false claims to a government agency, fraudulent demand for money presented to a government agency, filing a false or fraudulent tax return, and false statements to a government agency).

Under U.S. law, two principal provisions serve as the statutory bases for most export control prosecutions. Those provisions are (1) the Arms Export Control Act (AECA) and (2) the International Emergency Economic Powers Act (IEEPA). The AECA applies to the export of articles and services that are of exclusively military application. The IEEPA restricts the export of dual-use goods—items and

technology that have some commercial application but could also make a significant contribution to military programs. Specifically, by means of IEEPA, Congress granted authority to the President and the Department of the Treasury to issue orders and regulations that impose restrictions on transactions involving Specially Designated Nationals (SDNs). Such restrictions are based upon the threats posed by designated entities to the national security of the United States as a result of their involvement in, for example, terrorist activities or the proliferation of weapons of mass destruction. The process of adding a person to the SDN list involves comprehensive research and investigation (which can last a year or more), the development of an administrative record supporting government findings, the internal review of this record for legal sufficiency, and the coordination among various elements of the U.S. Government with further checks for sufficiency and accuracy.

The dual criminality treaty provision is intended to provide flexibility so that extradition is granted even though, as is often the case between two countries, the offenses that would be applied to the conduct in each state are not necessarily the same. As a point of comparison, the United States has a classification system for dual-use goods that is very similar (although not precisely the same) to that of the E.U. Aside from similar restrictions on military goods, the E.U. has implemented export controls on dual-use goods as well as restrictions upon entities involved in proliferation or terrorism. The reasoning behind this end-user based approach is that entities posing the greatest risk to global security can reap significant benefits from even the most modest assistance—whether such assistance is financial, technical, or involves the acquisition of material goods. This end-user based approach is largely effective because world governments and organizations recognize that enforcement personnel are not always in a position to make independent assessments regarding the strategic use of materials or to accurately gauge the threat posed to national security.

For example, E.U. Council Regulation No 423/2007, dated 19 April 2007, paragraph (6), used the Council's

> implementing powers . . . in view of the objectives of UNSCR [United Nation's Security Council Resolution] 1737 (2006), notably to constrain Iran's development of sensitive technologies in support of its nuclear and missile programmes, and the proliferation-sensitive nature of the activities undertaken by the persons and entities supporting these programmes.

Council Regulation 423/2007, para. 6, 2007 O.J. (Euratom). *See also* Council Regulation 423/2007, art. 7(2), 2007 O.J. (Euratom) (concerning restrictive measures against Iran). Much like the comprehensive U.S. system of SDNs, Article 7 of the E.U. Regulation does not delineate and control specific commodities based on strategic end-use but instead freezes all "funds and economic resources" relating to designated entities and prohibits all "funds or economic resources" from benefitting designated entities in Iran. *Id.*

IV. Framing the conduct in charging decisions

Export violations under U.S. law sound primarily in fraud because they involve a misrepresentation of the nature of a good, its end-use, or its end-user. In many instances, the violations are furthered through the illicit use of the financial system. Accordingly, in addition to export control violations, where applicable, offenders can and should be charged with money laundering, smuggling, defrauding the United States, and false statements—all offenses that are recognized in some form by treaty partners.

Referencing the E.U. system again for illustrative purposes, the U.S.-E.U. Extradition Agreement specifies that an offense shall be considered an extraditable offense

> in criminal cases relating to taxes, customs duties, currency control and the import or export of commodities regardless of whether the laws of the requesting and requested States provide for the same kinds of taxes, customs duties, or controls on currency or on the import or export of the same kinds of commodities.

Agreement on extradition between the European Union and the United States of America, 19.7.2003, art. 4 para. 3(c), 2003 O.J. (L 181) 29 (EU). This provision represents the proper analysis of dual criminality in such cases and, in fact, was deemed a necessary amendment only with respect to older treaties that authorize extradition exclusively with respect to a list of specified criminal offenses.

Although there are often attempts to introduce a political element to extraditions involving proliferation related crimes, they are not political offenses and should not be treated as such. If criminal conduct in the United States is charged in a way that fairly reflects the fraudulent nature of the conduct, more often than not, dual criminality should be achieved even if the goods, services, or technical data were not controlled by both countries in precisely the same way. Moreover, the offender need not have committed these violations while physically within the United States. If the offender directed or caused others to commit the violations, there should be a sufficient basis to determine that the offenses are extraditable. Similarly, in the case of prohibited or designated entities, a finding of dual criminality should not require the extraditing court to consider the strategic nature of the unlawfully exported goods or make a rudimentary damage assessment. When an offender has willfully defrauded the U.S. Government by false or fraudulent misrepresentations, the only consideration should be whether the entity was designated consistent with domestic national security authorities.

V. Conclusion

The illicit trade in arms and technology is a global problem and requires a global response. The United States has a critical part to play in addressing this problem, but is certainly not the only location in which proliferators shop for (or steal, increasingly, by cyber intrusion) weapons data and technology. Illicit procurement efforts span the globe and target many nations. Therefore, curbing illicit procurement requires a multi-national effort, with many nations and their intelligence and law enforcement agencies working together toward this common goal.

Export prosecutions involving extradition are not without some interesting challenges, and success is never a guarantee. However, to address the proliferation threat perpetuated beyond our borders, we must continue to take a network-based approach and, in pursuit of the network, prosecute offenders who are willfully violating U.S. law, even if they do so from afar. ❖

ABOUT THE AUTHOR

❑ **Ryan P. Fayhee** is the National Export Enforcement Coordinator for the Department of Justice's National Security Division, where he directs a national program to enhance the Government's ability to investigate and prosecute export control violations. Mr. Fayhee is on detail to the Department of Justice from the U.S. Attorney's Office for the Northern District of Illinois. Prior to his service as an Assistant U.S. Attorney, Mr. Fayhee was a Department of Justice trial attorney for eight years, most recently with the Counterespionage Section. Mr. Fayhee joined the Department of Justice through the Attorney General's Honors Program following a federal clerkship in the Central District of Illinois. ✠

Intelligence Specialist Support to Export and Embargo Prosecutions

Gregory Dunlap
Senior Intelligence Advisor
Counterespionage Section
National Security Division

I. Introduction

Shortly after the events of September 11, 2001, the Attorney General asked all Department of Justice (Department) components to assess their capacities to perform intelligence analysis and to institute procedures to improve intelligence capabilities, wherever necessary. As a result of the Attorney General's request, the Intelligence Specialist (IS) position was conceived, developed, funded, and integrated into the 93 U.S. Attorneys' offices (USAOs). In the first few years of their existence, ISs focused almost exclusively on activities related to counterterrorism. Before long, however, their unique skillsets were increasingly relied upon to provide analytic and other support to a variety of national security cases and activities, including those related to export and embargo enforcement.

Violations of export controls impact U.S. national security in a variety of ways. To cite several examples, unlawfully exported U.S. electronic components have been used in Improvised Explosive Devices employed by insurgents in Iraq to kill and maim U.S. service members, stolen International Traffic in Arms Regulations-controlled technical data has been exploited by China to accelerate their military programs, and highly-specialized metals fraudulently procured through subterfuge have made their way into Iran's uranium enrichment centrifuges. While the Department has made considerable headway in prosecuting export cases over the past five years, keeping pace with the volume of unlawful activity (and the pace at which it occurs) remains a challenge. The principal difficulty is rooted in the complexity of the cases, which typically take years to develop and successfully prosecute. Case complexity coupled with stagnant or dwindling budgetary resources has created an imperative for USAOs to fully leverage the capabilities of USAO ISs, the national USAO IS network, and, as needed, intelligence support provided by the Department's Counterespionage Section.

In a speech to the 2009 Intelligence Specialist Conference, Attorney General Holder stated, "[w]e expect you [ISs] to serve many critical roles . . . *you need to be intelligence advisors, information brokers, strategic and operational planners, and tactical analysts*." Attorney General Eric Holder, Speech to the Intelligence Specialist Conference (2009) (emphasis added). This article examines each of these IS roles and discusses how each role supports export and embargo enforcement. It also provides a brief list of recommended public and private export-related resources accessible online by USAO personnel.

II. Intelligence Specialist roles

A. Intelligence advisors

ISs are the USAOs' experts on intelligence matters and, wherever necessary, provide advice to prosecutors on intelligence-related issues. This support could be as simple as helping an attorney to decipher a classification caveat in an intelligence report or as complex and nuanced as providing case-related recommendations based on the analysis of evidence and intelligence information. An IS's comprehension of intelligence concepts and processes is particularly advantageous in export cases, which seldom progress through prosecution without intelligence issues arising, such as Foreign Intelligence

Surveillance Act evidence collection. Their knowledge, access to information, and ability to conduct in-depth unclassified and classified research and analysis makes an IS an invaluable resource that should be regularly consulted.

B. Information brokers

USAOs regularly generate and uncover intelligence while prosecuting export and embargo cases. For example, some of the information obtained from an email search warrant or proffer session could have little to no value in a prosecution, but the same information could greatly aid intelligence personnel mapping an Iranian procurement network or writing an assessment on Chinese military aircraft research and development. Unlike terrorism cases, which are led by the FBI and have well-established lines of communication for reporting valuable information to the Intelligence Community, export cases are typically investigated by agencies that lack intelligence support. ISs are uniquely qualified to identify, analyze, and share pertinent information derived from these cases to appropriate investigative agencies, other USAOs, the Department, and the Intelligence Community.

ISs can also serve as conduits for information flowing from partner agencies to the USAO. For example, a prosecutor might be looking for information on the possible end-uses of a particular widget that was unlawfully exported to a sanctioned entity. While the IS is capable of conducting his or her own research, another agency may have the time and even specialized expertise relating to the technology in question. ISs regularly liaise with personnel throughout the law enforcement and intelligence communities, and, as a result, they know which partner agencies' resources, capabilities, and information can and should be leveraged to support the prosecutor's request.

C. Strategic and operational planners

Strategic and operational planning (and analysis) is an important capability that USAOs need for a variety of purposes, specifically, developing district-wide priorities and goals, identifying gaps in resource allocation, evaluating individual and connected cases, and guiding prosecutorial decisions. Averaging more than 20 years of experience, ISs have the knowledge, skills, and tools to offer valuable support to any segment of the planning and analytic process. In the context of export enforcement for example, an IS can identify particular items being sought by a priority country of interest through open-source and classified research and cross-reference them with known manufactures, suppliers, or defense contractors in their district. After a thorough analysis of the results, ISs can provide prosecutors with a road map to set priorities and focus investigators.

D. Tactical analysts

For purposes of this article, tactical analysis refers to providing support in individual cases through objective research and structured analysis. It is important to note that this is not the type of intelligence support that results in a voluminous summation of homeland security threats or an assessment containing terms such as "believe," "assess," "likely," and "probably." At its heart, tactical analysis is designed to provide attorneys with unvarnished and unbiased in-house support, typically in response to case-related questions that require the researching, filtering, collating, and summarizing of information and intelligence of value. For example, an IS might locate and assemble relevant and well-sourced information on a particular Iranian government entity for use in a sentencing memorandum, or review and analyze evidence from a case and, through the use of analytic software, create a link diagram of a network or a timeline of events.

Other examples of tactical analysis include identifying intelligence gaps to help guide further investigation, preparing appropriate intelligence products, identifying and assisting in reviewing classified materials for Federal Rule of Criminal Procedure Rule 16 discovery and *Brady* and Jencks Act material, and researching and monitoring local, regional, and national intelligence systems for information that

could impact investigations or prosecutions. Unlike traditional intelligence analysis, the value of which may be lost on some attorneys, tactical analysis gets to the heart of prosecutors' primary mission—to efficiently and successfully prosecute those guilty of unlawful behavior.

III. Online resources

ISs have access to a variety of online resources to support research efforts. The following is a short list of links to publicly and privately available online resources that consistently provide valuable information for use in export and embargo cases.

A. Wisconsin Project

- Found at http://www.wisconsinproject.org/
- Conducts research and advocacy to stem the spread of nuclear and other weapons of mass destruction
- Its three principal products are Risk Report database, Iran Watch, and Iraq Watch (links available on main Web page).

B. The Risk Report

- Found at https://rrdb.riskreport.org/
- Subscription database that catalogs unclassified information on companies and designated foreign nationals around the world who are suspected of links to weapons of mass destruction programs or to terrorism, as well as photographs and information on the parts and components used in WMD applications
- Contact CES for login information.

C. Open Source Center

- Found at http://www.opensource.gov
- Provides information on foreign political, military, economic, and technical issues and contains sources from more than 160 countries in more than 80 languages and hosts content from several commercial providers
- Government employees can obtain an account by clicking on the account registration link on the main Web page.

D. Institute for Science and International Security

- Found at http://www.isis-online.org/
- A non-profit, non-partisan institution dedicated to informing the public about science and policy issues affecting international security
- Provides analysis related to nuclear programs in states that seek or possess nuclear weapons

E. Defense and Export-Import Update

- Distributed via email
- Daily export-related newsletter from Gary Stanley, Global Legal Services, PC
- To subscribe, email your name, title, company, and email address to gstanley@glstrade.com.

F. The Export Practitioner

- Found at http://www.exportprac.com/
- Subscription-based service that provides news and analysis on export licensing and enforcement
- Contact CES for access assistance.

G. Export Enforcement Coordination Center

- Found at http://www.ice.gov/export-enforcement-coordination-center/
- Created by Executive Order 13558, the Center's primary mission is to de-conflict export and embargo cases.
- Contact CES for information on how to submit de-confliction requests for export matters in your district.

H. Other important Web sites

- Department of Commerce, Bureau of Industry and Security, http://www.bis.doc.gov/
- Department of State, Directorate of Defense Trade Controls, http://www.pmddtc.state.gov/
- Department of the Treasury, Office of Foreign Assets Control, http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx
- Consolidated Export Screening Lists, http://www.export.gov/ecr/eg_main_023148.asp. This site includes all lists of designated foreign nationals, denied parties, and other entities with which transactions by U.S. persons are prohibited or require a license or Government approval.

IV. USAO Counter-proliferation Intelligence Working Group

In 2010, the Executive Office for U.S. Attorneys IS Program Manager, in partnership with the Department's Counterespionage Section, established the Counter-proliferation Intelligence Working Group (CPIWG). Its mission is to develop and provide actionable all-source intelligence solutions to support the investigation and prosecution of cases affecting national security and the export of military/strategic commodities and dual-use technology to sanctioned countries and designated entities. For further information on how the CPIWG can provide assistance to one of your matters, please contact the EOUSA IS Program Manager or CES Senior Intelligence Advisor.

V. Conclusion

The roles described in this article may not perfectly align with the capabilities of every IS. Similarly, each activity may not be applicable or needed in every district. As an initial step however, prosecutors should take some time to get to know their district IS—What is their background? What are their skills? What data sources can they access? Once this baseline relationship has been established, prosecutors should hopefully be able to answer the basic interrogatives relating to their IS and their skillset. Building upon this foundational understanding, the prosecutor and the IS can then work together to tailor mutually beneficial advisory and analytic support. If properly engaged and utilized, ISs can greatly benefit a prosecutor's case, the USAO's mission, and significantly improve the Department's overall ability to disrupt, neutralize, and prosecute unlawful export activities.❖

ABOUT THE AUTHOR

❑ **Gregory Dunlap** is a Senior Intelligence Advisor in the Department of Justice, National Security Division, Counterespionage Section. He started his intelligence career in the U.S. Army, specializing in counterintelligence and Human Intelligence source operations overseas, including Afghanistan, Bosnia, Iraq, and Uzbekistan. As a Department of Defense civilian, Mr. Dunlap served as a counterterrorism analyst and Middle East and Southwest Asia Specialist. He joined the Department of Justice in 2006, first working as an Intelligence Specialist in the U.S. Attorney's Office for the District of Alaska, and later as the Intelligence Program Manager for the 93 U.S. Attorneys' offices, where he was responsible for all program planning, direction, training, and evaluation. ✠

The *United Technologies* Case: Investigating and Prosecuting a Major Defense Contractor Following a Voluntary Disclosure of Unlawful Exports to an Embargoed Nation

Stephen B. Reynolds
Deputy Chief/ATAC Coordinator
National Security and Major Crimes Unit
District of Connecticut

I. Introduction

Preventing the loss of controlled technology is critical to protecting our national security. Foreign actors, whether state-sponsored or otherwise, are routinely and actively targeting sensitive research and development data and intellectual property from universities, government agencies, and private industry, in order to exploit that material for their own purposes. All too often the foreign actor is a nation subject to the United States' arms embargo, and their suppliers, unwittingly or not, are United States defense contractors.

If and when controlled defense technology is released to an embargoed nation in violation of our export laws and regulations, it is critical that the individuals or corporations involved make timely and accurate disclosures to the U.S. Government—indeed, they are *required* to do so. For approximately 25 years, federal law has required that individuals or companies that know about the unlawful export or transfer of defense articles and technical data to embargoed nations such as China, Iran, North Korea, and Syria, must disclose such violations to the Department of State (DOS), which regulates such exports or transfers. *See* 22 U.S.C. § 2778(c) (2013); 22 C.F.R. § 126.1(a), (e) (2013). Our national security and

ability to prepare is strengthened when we know about defense materials that have been unlawfully provided to our potential adversaries.

An affirmative legal duty upon a corporation to disclose its own legal violations to the U.S. Government is rare, and the imposition of criminal liability for such a failure is, appropriately, even more rare. Where a company makes a voluntary disclosure of its own legal violations, and in those rare instances where a criminal investigation ensues, we must tread carefully as we encourage and rely on our defense contractors to make timely and accurate voluntary disclosures. We also do not want to cause a chilling effect on such disclosures. Where, however, willful exports of defense technology to an embargoed nation have occurred, and where a corporation willfully fails to make a timely disclosure, or willfully makes materially false or misleading statements or omissions in such a disclosure, individuals and corporations have fair notice that such violations may be investigated and prosecuted criminally.

This article discusses these issues in the context of a recent case, *United States v. United Technologies Corp., Hamilton Sundstrand Corp. and Pratt & Whitney Canada Corp.*, 3:12CR146 (WWE) (D. Conn. June 28, 2012), which involved unlawful exports of U.S.-origin software and belated and materially misleading disclosures to the U.S. Government.

II. Summary of the case

In June 2012, Pratt & Whitney Canada Corporation (PWC), a Canadian subsidiary of the Connecticut-based defense contractor United Technologies Corporation (UTC), pled guilty to violating the Arms Export Control Act and making false statements in connection with PWC's illegal export to China of U.S.-origin software that was used in the development of China's first modern military attack helicopter, the Z-10. UTC, Hamilton Sundstrand Corporation (HSC), and PWC agreed to pay more than $75 million as part of a global settlement with the Department of Justice (DOJ), the U.S. Attorney's Office for the District of Connecticut, and the DOS in connection with the export violations and for making belated and misleading disclosures to the U.S. Government about the illegal exports. As part of the global resolution, the companies also admitted to more than 500 export violations and were required to retain an independent monitor to assess their compliance with an extensive remedial action program over the next several years. The combination of the guilty pleas, $75 million in penalties, and extensive corrective actions was one of the largest resolutions of export violations against a major defense contractor in DOJ history, and both the case and the efforts that UTC has made, and continues to make, to ensure robust trade compliance have had positive and far-reaching implications for export compliance throughout the defense industry as a whole.

III. The export scheme

Since 1989, the United States has imposed a prohibition upon the export to China of all U.S. defense articles and associated technical data as a result of the conduct in June 1989 at Tiananmen Square by the military of the People's Republic of China. In February 1990, the U.S. Congress codified the embargo, imposing a prohibition upon licenses or approvals for the export of defense articles to the People's Republic of China. Among other things, helicopters and associated hardware and technical data were specifically named for inclusion in the ban.

Dating back to the 1980s, China had been seeking to develop a military attack helicopter. Beginning in the 1990s, after Congress imposed the prohibition on exports to China, China sought to develop its attack helicopter under the guise of a civilian medium helicopter program in order to secure Western assistance. The Z-10, developed with assistance from Western suppliers, ultimately became China's first modern military attack helicopter.

During the development phases of China's Z-10 program, each Z-10 helicopter was powered by engines supplied by Canadian-based PWC. PWC delivered 10 of these development engines to China in

2001 and 2002. During the development phases of the project, PWC knowingly and willfully caused HSC to export technical data from the United States to China—namely, certain electronic engine control software—without having first obtained a license for such exports from DOS. Specifically, in 2002 and 2003, PWC caused six versions of the software to be electronically transmitted—and therefore, exported—from HSC in the United States to PWC in Canada, and then to China, where it was used in the PWC engines for the Z-10.

PWC knew from the start of the Z-10 project in 2000 that China was developing an attack helicopter and that supplying it with U.S.-origin components would be illegal. In one internal email, a PWC manager stated, "We must be very careful that the helicopter programs we are doing with the Chinese are not presented or viewed as military programs. As a result of these sanctions, we need to be very careful with the Z10C program. If the first flight will be a gun ship then we could have problems with the US government." *See* Deferred Prosecution Agreement, Appendix A—Statement of Facts at 7, Doc. #5, *United States v. United Technologies Corp., Hamilton Sundstrand Corp. and Pratt & Whitney Canada Corp.*, 3:12CR146 (WWE) (D. Conn. June 28, 2012) (hereinafter "Statement of Facts").

When the Chinese claimed, in light of these issues, that a civil version of the helicopter would be developed in parallel, PWC marketing personnel expressed skepticism internally about the "sudden appearance" of the civil program, the timing of which they questioned as "real or imagined." PWC nevertheless saw an opening for PWC "to insist on exclusivity in [the] civil version of this helicopter," and stated that the Chinese would "no longer make reference to the military program." PWC failed to notify UTC or HSC about the attack helicopter application until years later and purposely turned a blind eye to the helicopter's military application. *See* Statement of Facts at 5.

HSC in the United States believed it was providing its software to PWC for a civilian helicopter in China, based on claims from PWC. By early 2004, however, HSC learned that there might be an export problem and stopped working on the Z-10 project. UTC also began to ask PWC about the exports to China for the Z-10. Regardless, PWC on its own modified the software and continued to export it to China through June 2005.

PWC's illegal conduct appeared to be driven by profit. PWC anticipated that its work on the Z-10 military attack helicopter in China would open the door to a far more lucrative civilian helicopter market in China, which according to PWC estimates, was potentially worth as much as $2 billion to PWC.

IV. Belated and misleading disclosures to the U.S. Government

The companies failed to disclose to the U.S. Government the illegal exports to China for several years and only did so after an investor group queried UTC in early 2006 about whether PWC's role in China's Z-10 attack helicopter might violate U.S. laws. The companies then made an initial disclosure to the DOS in July 2006, with follow-up submissions in August and September 2006.

The 2006 disclosures contained several false or materially misleading statements. Among other things, the companies asserted that they were unaware until 2003 or 2004 that the Z-10 program involved a military helicopter. In fact, by the time of the disclosures, all three companies were aware that PWC officials knew at the project's inception in 2000 that the Z-10 program involved an attack helicopter.

Today, the Z-10 helicopter is in production and initial batches were delivered to the People's Liberation Army of China in 2009 and 2010. The primary mission of the Z-10 is anti-armor and battlefield interdiction. Weapons of the Z-10 have included 30 mm cannons, anti-tank guided missiles, air-to-air missiles, and unguided rockets.

V. The investigation and charges

The investigation and prosecution of UTC, PWC, and HSC stretched over several years and investigating the conduct—particularly given the belated and misleading disclosures—necessitated substantial time, effort, and resolve. The case presented significant challenges, including navigating complicated assertions of corporate privilege, conducting in-depth interviews of numerous domestic and foreign witnesses, and reviewing voluminous corporate documents and emails, much of which involved highly technical data. The case also involved complex and extensive negotiations with the UTC entities and sophisticated corporate defense counsel during both the investigative and prosecution phases.

Ultimately, in June 2012, the U.S. Attorney's Office for the District of Connecticut filed a three-count information charging UTC, PWC, and HSC. Count One charged PWC with violating the Arms Export Control Act in connection with the illegal export of the engine control software to China for the Z-10 helicopter, in violation of 22 U.S.C. § 2778(b)(2) and (c), 18 U.S.C. § 2, and 22 C.F.R. §§ 127.1(a) and 127.3. Count Two charged UTC, PWC, and HSC with making false statements to the U.S. Government in their belated disclosures relating to the illegal exports, in violation of 18 U.S.C. § 1001. Count Three charged PWC and HSC with failure to timely inform the U.S. Government of exports of defense articles to China, in violation of 22 U.S.C. § 2778(c) and 22 C.F.R. § 126.1(a) and (e).

While PWC pled guilty to Counts One and Two, prosecution of UTC and HSC on Count Two and PWC and HSC on Count Three was deferred for two years, in light of extensive remedial actions that the companies had taken to date, their entry into a separate and independent Consent Agreement with the DOS, and their willingness, as set forth in a deferred prosecution agreement, to (1) continue their corrective actions and undertake additional remedial actions, (2) acknowledge responsibility for their behavior, (3) continue their cooperation with governmental regulatory agencies, and (4) demonstrate their future good conduct and full compliance with export laws and regulations.

UTC, PWC, and HSC—as part of the global resolution involving the U.S. Attorney's Office for the District of Connecticut, the DOJ, and a consent agreement with the DOS—also admitted to more than 500 additional export violations, agreed to an independent monitor for two years, and paid more than $75 million in fines, forfeiture, and penalties. This agreement is one of the largest resolutions of export violations against a major defense contractor in DOJ history.

VI. Takeaways

There are a number of "takeaways" from the UTC case that may be more broadly applied in the investigation and prosecution of other export cases.

First, it is helpful to bear in mind that export violations not only involve the unlawful transfer of defense articles, weapons, munitions, and other military hardware, but also can involve the unlawful transfer of technical data. Safeguarding controlled defense technology and investigating and prosecuting illegal transfers of technical data can be just as important as investigating and prosecuting the unlawful export of weapons, night vision systems, and the like—particularly where our adversaries are so aggressively seeking to obtain our defense technology to exploit for their own use and military development.

Second, a voluntary disclosure does not necessarily preclude a criminal investigation and prosecution. Where an individual or entity makes a timely and truthful voluntary disclosure of an export violation, such a disclosure can—and most often should—be a safe harbor for a number of reasons. As noted above, we count on our defense contractors to be good corporate citizens and to make voluntary disclosures, and we do not want to cause a chilling effect on such disclosures. Such disclosures also enhance our national security and preparedness by informing the U.S. Government when defense materials have been unlawfully provided to our potential adversaries. All of this depends, however, on the integrity of the voluntary disclosure system and its participants. Accordingly, in those rare instances

where exports of defense technology to an embargoed nation have occurred, and where a corporation may have willfully failed to make a timely disclosure or willfully made materially false or misleading statements or omissions in such a disclosure, such violations should be investigated for potential criminal liability.

Third, the UTC case was the first time that defendants were charged with failing to timely disclose illegal exports to an embargoed nation. The Government, however, exercised its prosecutorial discretion and included that charge in the deferred prosecution portion of the case, rather than in the guilty plea and conviction portion of the matter, given that the regulation imposing the affirmative duty to disclose had not previously been criminally charged in its 25 years of existence. By doing so, however, the Government provided fair and open notice to defense contractors and others that, in the future, knowing and willful violations of the affirmative duty to make a timely disclosure of the unlawful export of defense articles and technology to embargoed nations may be prosecuted criminally. Accordingly, prosecutors should be aware that a failure to timely disclose an unlawful export to an embargoed nation may serve as a possible basis for a criminal investigation and prosecution. Moreover, defense contractors would be well advised, upon learning of an export of defense articles or technology to an embargoed nation, to promptly inform the DOS of the potential violation, even as it continues to conduct an internal investigation.

Fourth, the UTC case helps to highlight the fact that some common misperceptions and challenges that frequently arise in export cases may be overcome. For example, criminal guilty pleas by defense contractors and corporations are entirely possible, without causing irreparable harm to existing defense contracts, national security, and military operations, which can be carved out and, notwithstanding potential debarment issues, can be successfully navigated. The case also underscores the fact that foreign individuals and corporations may be successfully prosecuted and convicted notwithstanding common misperceptions that we will "never get them." Not only has the DOJ had a number of recent successes in getting individuals extradited to the United States to face export violation charges, but individuals and corporations, both domestically and abroad, who hope to continue to do business with the U.S. defense industry and engage in international trade have a tremendous incentive to cooperate with a criminal investigation and prosecution. In the UTC case, UTC, HSC, and Canadian-based PWC voluntarily cooperated with the Government's investigation, willingly producing foreign witnesses and documents that otherwise would have had to take place through MLAT procedures. Finally, even if the Government is unsuccessful in extradition efforts, a criminal prosecution and indictment may well trigger other appropriate consequences, such as debarment, export denial designation, or practical restrictions on travel to the United States or on international travel if an arrest warrant and red notice is lodged with Interpol.

VII. Conclusion

The UTC case demonstrates that Assistant U.S. Attorneys (AUSAs) are not alone when forging into what many AUSAs understandably consider to be a complicated and highly technical area of the law. Not only are there outstanding law enforcement agents from the FBI, DHS, DCIS, Commerce, and other agencies who are well versed in export enforcement, but there are excellent trial attorneys and supervisors in the National Security Division's Counterespionage Section who not only are subject matter experts and add value in the investigation and prosecution of export cases, but also stand ready to assist with as much or as little support and assistance as a particular district needs.

Safeguarding our controlled technology is vital to our national security interests both at home and abroad. Foreign governments are actively seeking U.S. defense technology for their own military development. AUSAs, with the assistance of the Counterespionage Section, play a critical role in protecting our defense technology by holding accountable those who willfully violate our export laws and regulations, which in turn strengthens export compliance and deters future violations.❖

ABOUT THE AUTHOR

❑ **Stephen B. Reynolds** serves as the ATAC Coordinator and Deputy Chief of the National Security and Major Crimes Unit for the U.S. Attorney's Office for the District of Connecticut, where he has been a federal prosecutor since 2002. From 2008 to 2012, Mr. Reynolds was among those who handled the investigation and prosecution of *United Technologies Corporation, Hamilton Sundstrand Corporation, Hamilton Sundstrand Corporation and Pratt & Whitney Canada Corporation* case. Mr. Reynolds has served as a frequent faculty member at DOJ national security courses in Washington, DC and at the National Advocacy Center in Columbia, South Carolina. Prior to joining the U.S. Attorney's Office, Mr. Reynolds worked in private practice at Day, Berry and Howard in Hartford, Connecticut, and also served as a law clerk in Bridgeport, Connecticut to U.S. District Court Judges Stefan R. Underhill and Alan H. Nevas. ✠

The Prosecution of Chitron Electronics, Inc.: How We Identified, Prosecuted, and Dismantled a Chinese Front Company Hiding in the United States

B. Stephanie Siegmann
Assistant United States Attorney
Anti-Terrorism and National Security Unit
District of Massachusetts

Since the 1990s, the People's Republic of China (PRC) has been increasingly focused on acquiring U.S. technology, both military (defense articles) and dual-use technology, which can be used to advance its military capabilities and enhance the quality of its military operations. *See* SELECT COMMITTEE, HOUSE OF REPRESENTATIVES, REPORT OF THE SELECT COMMITTEE ON U.S. NATIONAL SECURITY AND MILITARY/COMMERCIAL CONCERNS WITH THE PEOPLE'S REPUBLIC OF CHINA (THE COX COMMISSION REPORT), xiii (1999), *available at* http://www.gpo.gov/fdsys/pkg/GPO-CRPT-105hrpt851/pdf/GPO-CRPT-105hrpt851.pdf. Such activities pose a serious national security threat to the United States and allied regional military forces. For instance, the PRC's acquisition of sophisticated military electronics could allow it to defeat U.S. weapon systems. In addition to other methods of illegal procurement (for example, espionage, procurement networks in third countries, disguising military acquisitions as commercial in nature, etc.), the PRC uses front companies established by PRC nationals in the United States (as well as in other countries) to illegally and covertly obtain U.S. technology, equipment, and information for the PRC government. In 2005, the FBI Assistant Director for Counterintelligence estimated that approximately 3,000 Chinese front companies were operating in the United States. *See* FBI SPY CHIEF ASKS PRIVATE SECTOR FOR HELP, *available at*

http://www.cnn.com/2005/US/02/10/fbi.espionage/; *see also* DALLAS BOYD ET AL., DEFENSE THREAT REDUCTION AGENCY: ADVANCED TECHNOLOGY ACQUISITION STRATEGIES OF THE PEOPLE'S REPUBLIC OF CHINA 38 (2010).

The Government has not publicly released any new or more recent estimates of this threat. What is clear from the criminal prosecutions brought around the country, however, is that this threat has not abated. To the contrary, it has expanded. The numbers of individuals and companies that are working within our borders to smuggle goods to the PRC have increased, and their methods of illegal acquisition have grown more sophisticated. *See, e.g.*, AMERICA'S NEW THREAT: CHINA'S SPIES, *available at* http://www.boston.com/news/nation/articles/2011/05/07/ap_impact_chinas_spying_seeks_secret_us_info.

For example, in late 2007, investigators identified Chitron Electronics, Inc. (Chitron-US), a small company incorporated in Waltham, Massachusetts, as a front company that was being used to illegally procure export-controlled U.S. technology for entities located in mainland China, primarily Chinese military research institutes. In 2009, Chitron-US; its Chinese parent company, Chitron Electronics Company Limited, headquartered in Shenzhen, China; Zhen Zhou Wu (Wu); and his ex-wife, Yufeng Wei (Wei), were charged in a 34-count indictment with conspiring to violate the U.S. export laws and committing numerous export violations, after an extensive joint investigation by federal agents of the Department of Commerce, Office of Export Enforcement, Department of Homeland Security's Homeland Security Investigation, Defense Criminal Investigative Service, and the FBI. In 2010, after a six-week trial, Chitron-US, Wu, and Wei were each convicted of illegally exporting numerous electronic components from the United States or committing numerous violations of U.S. export laws and conspiring with each other and others to illegally export military and sophisticated electronics to China over a period of 10 years, in violation of the Arms Export Control Act (AECA), International Traffic in Arms Regulations (ITAR), and Export Administration Regulations (EAR).

The purpose of this article is to suggest ways to prosecute other companies engaged in activities designed to circumvent U.S. export laws, dismantle their illegal procurement network, and effectively punish the criminally culpable parties.

I. Background

Wu and Wei, both Chinese nationals, pursued graduate degrees in the United States after getting married in China. In 1996, Wu returned to the PRC to found Chitron-Shenzhen, a distributor of U.S.-made electronics components in China. Over the period of the next 11 years, Wu transformed this company into a multi-million dollar enterprise that specialized in the procurement of U.S. manufactured military parts for Chinese customers. By 2007, Chitron-Shenzhen had opened five branch offices—three in mainland China, one in Hong Kong, and one in the United States (Chitron-US). Chitron-Shenzhen's major customer was the Chinese military. *See generally United States v. Wu*, 711 F.3d 1, 8–11 (1st Cir. 2013) (Chitron-Shenzhen specialized in military and industrial parts, and Wu presented himself to customers as an export compliance expert with a specialty in military products.).

In 1996, after he founded Chitron-Shenzhen and learned about U.S. export laws and the difficulties of exporting electronics directly from the United States to the PRC, Wu arranged for his then-wife, Wei, who was living in the United States pursuant to a student visa, to open a purchasing office for Chitron-Shenzhen in the United States. Wei ran the purchasing office, called "Perfect Science and Technology," for two years as a sole proprietorship under her own name.

In 1998, Wu incorporated Chitron Electronics, Inc., as a Massachusetts corporation to serve as the United States branch office of Chitron-Shenzhen. Chitron-US replaced Perfect Science and Technology as Chitron-Shenzhen's purchasing office in the United States. After incorporating Chitron-US, Wu served as its president, but spent the majority of his time at the Shenzhen office controlling and overseeing the company's entire operation. Wei worked at Chitron-US' office in Massachusetts as its office manager and

oversaw the purchase of parts from vendors in the United States and the shipment of those parts to Chitron's customers in China. Once a year, Wu traveled to the United States to visit Chitron-US and he remained in daily contact with Wei throughout the year, coordinating the activities of Chitron-US through electronic tasking lists and an online database system. Under the direction and control of Wu and Wei, each year Chitron-US purchased tens of thousands of parts from U.S. suppliers, worth tens of millions of dollars, and exported them to China.

To circumvent U.S. export laws, Wu instructed Wei and the few U.S. employees eventually hired at Chitron-US not to tell U.S. companies that the parts they were ordering were going overseas. Rather, at Wu's instruction, Wei and employees at Chitron-US told U.S. suppliers to ship the ordered parts to Chitron-US' Massachusetts office. Upon receipt of the ordered products at Chitron-US, its employees, under Wei's supervision, packed and consolidated the items into boxes and, at the instruction of Wu, exported the products to Chitron-Shenzhen (located in mainland China) through Hong Kong, without obtaining the required export licenses from the Department of State and Department of Commerce. The exported equipment included military electronics and sensitive export restricted technology used in electronic warfare, military radar, fire control, missile applications, and satellite communications.

Nearly all of Chitron-Shenzhen's customers were located in mainland China. Wu targeted military customers and promoted himself as an expert in military products. In 2002, Wu hired an engineer and traveled to Chinese military factories with this engineer to increase Chitron's business with the Chinese military. By 2007, Wu's efforts had succeeded. Chitron's major customers were China's military and aerospace industries. Indeed, Chitron procured and sold thousands of electronics components to research institutes of the China Electronics Technology Group Corporation (CETC). According to the Government's expert at trial, CETC procures, designs, and manufactures electronic components for the entire range of the Chinese defense industry. CETC provides "electronic components, semiconductors, integrated circuits, communication systems for the Chinese armed forces, Air Forces, Naval forces, and space/nuclear program." Testimony of Lt. Col. Shawn Bateman, AF, May 5, 2010, at 86–88. Furthermore, based on documents obtained from a search warrant executed at Chitron-US, employees at Chitron-Shenzhen tasked employees at Chitron-US on a regular basis to procure military parts, including items that were described in internal documents as parts for an army guided missile, parts for a sensitive military device, parts for military factories, parts for a military unit, and parts for military equipment.

Until 2005, Chitron-US would ship Chitron-Shenzhen's orders to freight forwarders in Hong Kong, who then repackaged the items and sent them to Chitron-Shenzhen, where the parts were inspected and sent to their customers in the PRC. In 2005, Wu established a one-room branch office in Hong Kong, Chitron-HK, to handle the increased business. This office was staffed by a single part-time employee who traveled to Hong Kong a few days a week while working full-time at Chitron-Shenzhen. After Wu opened this office, all of Chitron-US' shipments were sent to Chitron-HK rather than using other freight forwarders in Hong Kong. Chitron-HK, however, handled the shipments in the exact same fashion as the freight forwarders it had replaced—the U.S. packages were repackaged and forwarded to Chitron-Shenzhen for delivery to the end-users in mainland China.

Wu designed his illegal scheme around a loophole in U.S. export laws involving the treatment of Hong Kong as a separate country from the PRC. In 1997, after being ruled for more than 150 years by the British, the sovereignty over Hong Kong reverted back to the PRC. Despite this change in government control, the United States continues to treat the Hong Kong Special Administrative Region (Hong Kong) as a separate country from the PRC under its export laws. As a result, many items that require an export license from the Department of Commerce to be shipped to the PRC do not similarly require an export license to be shipped to Hong Kong. Furthermore, the Arms Embargo imposed against the PRC does not include Hong Kong even though Hong Kong is part of the same country and controlled by the same government. As a result of this disparate treatment, Hong Kong is often used as a transshipment point to evade U.S. export laws.

Before exporting parts from the United States, a Chitron-US employee prepared shipping documents for UPS, which in turn used the documents to prepare Shipper's Export Declarations (SEDs) on Chitron-US' behalf. The Department of Commerce requires every exporter to file a SED for any export of commodities valued at or above $2,500, or for which an export license is required. This document requests information regarding the identities and addresses of the U.S. shipper/exporter, the ultimate consignee/end-user, and any intermediary consignee or forwarding agent, as well as the country of ultimate destination, the export route including ports of export and unloading (import), and a complete description of the item(s) being shipped, including their value, export control classification number, and applicable export license numbers. The agent of the exporter or shipper is required to certify that the information provided in the SED is true and correct.

Chitron-US did not prepare individual shipping documents for each commodity being shipped. Instead, it prepared a list of parts in each package in the form of an invoice that was addressed to the Hong Kong freight forwarder and later Chitron-HK. On the shipping documents, which were primarily completed or reviewed by Wei, the parts being shipped were always described as "NLR" (no license required), the ultimate destination for the parts was always described as Hong Kong, and Chitron-US' freight forwarder in Hong Kong was always listed as the ultimate consignee (for example, the Hong Kong company hired for that purpose or Chitron-HK). Furthermore, Chitron-US never individually identified the export control classification number or U.S. Munitions List category of any specific part on their shipping paperwork. Indeed, in the case of the more than 25 charged illegal exports, Wei described the ITAR and EAR controlled goods simply as "NLR." (As described below, the defendants contended they did not know the charged parts were controlled and with regard to the EAR-controlled goods, they claimed that an exception to the license requirement applied.) On multiple occasions, Wei also undervalued the goods Chitron-US shipped to eliminate the SED filing requirement.

Beginning in 2003, Chitron-US' employees began expressing concerns to Wu and Wei that their activities violated U.S. export laws and that a large number of the parts Chitron's Chinese customers were seeking to procure were export restricted. Both Wu and Wei repeatedly disregarded these concerns. In 2005, Wei even laughed off the concern of three of her employees that they could be arrested and go to jail for their export activities. Rather than changing their policies, Wu stressed the importance of obtaining the parts from U.S. vendors and lying to them about where the parts were going.

As the number of these complaints increased, the number of tasks assigned to employees of Chitron-US decreased and so did their compensation, forcing at least one of their primary employees to quit. Thus, rather than relying upon Chitron-US to obtain quotes and place orders, in 2005, Wu established a buying department at Chitron-Shenzhen that would communicate directly with U.S. companies on a regular basis, using an 800 phone number designed to mask the fact that the employees were calling the U.S. companies from China. Similarly, using electronic mail, employees of Chitron-Shenzhen frequently represented to U.S. companies that they were working out of Chitron's U.S. office when in fact those employees were located in the PRC.

Despite the changes in the location of the employees who obtained quotes and placed orders, the method of shipment remained the same—U.S. vendors were instructed to ship the parts to Chitron-US where they were consolidated and exported to Chitron-Shenzhen through Hong Kong. By so doing, Wu and Wei were able to circumvent U.S. export laws for over 10 years.

II. Moving past mere suspicion

In 2007, the Government received information that strongly suggested Chitron-US was shipping military electronics to China in violation of the AECA and U.S. Arms Embargo. Upon receiving this information about a potential threat to our national security, the investigators and prosecutors worked quickly to come up with a plan to disrupt this procurement network. We quickly determined that Chitron-US had lied on hundreds of SEDs filed on their behalf with the Department of Commerce when it

indicated that the final end-user for the parts being exported was either a named freight forwarding company in Hong Kong or Chitron-HK, which acted as a freight forwarder for Chitron-US. These violations then served as the basis to initially charge Wu (upon his next scheduled visit to the United States) and Wei, and to execute search warrants at Chitron-US' office and Wei's residence.

After numerous search warrants were executed and more than three terabytes of data were seized, the Government faced a daunting challenge: how to prove that some of Chitron's millions of exports were illegal and that Chitron's employees knew such exports were illegal. Review of each part was simply not feasible. Thus, we decided to focus on the parts that were manufactured by defense contractors (businesses that develop products for, and provide services to, the U.S. military). Using the shipping records we obtained from UPS (Chitron-US' primary freight forwarder to Hong Kong), we quickly learned that Chitron had shipped parts manufactured by several defense contractors and a few other companies that were known for developing sensitive technology in the United States. We then contacted those manufacturers and asked them to provide a list of their export controlled parts. Using Chitron's shipping records and the manufacturers' lists of export restricted parts, the investigators were able to identify numerous exports that we believed violated U.S. export laws.

The next hurdle was proving that Chitron was told that the parts were indeed export restricted—required an export license to ship them to China—and that Chitron's management decided to export them without the required licenses. Because Chitron-US instructed U.S. manufacturers and distributors to ship parts to Waltham rather than Hong Kong or mainland China (as described above, Wu and Wei disguised the fact that they were exporting to China and made their transactions look like domestic sales), there was no obligation for the U.S. seller/distributor to notify Chitron of any applicable export restrictions for the goods sold and shipped to Massachusetts. Luckily, many of the distributors with whom Chitron transacted business did in fact notify agents of Chitron that the parts it was seeking to obtain, and had obtained, were export restricted under either the U.S. Munitions List (USML) or the Commerce Control List (CCL). These distributors listed the specific category under the USML or Export Control Classification Number under the CCL that applied to the part on their price quotes, invoices, packing lists, and shipping paperwork. They also included an export license disclaimer on their paperwork. Most often these disclaimers indicated that the export of the parts "may require a license."

III. The prosecution

A. The applicable export laws and regulations

There are two primary export control regimes: (1) the AECA, and its implementing regulations, ITAR, and (2) the EAR.

Although the EAR's authorizing statute, the Export Administration Act of 1979 (EAA), 50 U.S.C. App. §§ 2401–2420, expired on August 20, 2001, the EAR has been continued in full force and effect through periodic reauthorizations and successive invocations of the International Emergency Economic Powers Act (IEEPA). On August 17, 2001, President Bush issued Executive Order 13222, 66 Fed. Reg. 44025, 44025 (Aug. 17, 2001), in which he ordered that all provisions of the EAR "remain in full force and effect" under the authority of IEEPA. Executive Order 13222 has been extended by successive Presidential Notices, the most recent being that of August 8, 2013. *See* Continuation of the National Emergency With Respect to Export Control Regulations, 78 Fed. Reg. 49107, 49107 (Aug. 8, 2013).

Because the EAA has expired and the President annually continues the enforcement of the EAR by executive order, a violation of the EAR is prosecuted using IEEPA. *See United States v. Wu*, 711 F.3d 1, 21 (1st Cir. 2013). IEEPA makes it illegal to violate, attempt to violate, or conspire to violate, any license, executive order, or regulation. *See* 50 U.S.C. § 1705(a) (2013) ("It shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or

prohibition issued under this chapter."). In 2007, Congress enacted an anti-smuggling statute, 18 U.S.C. § 554, that may also be used to prosecute violations of both the EAR and the ITAR. Section 554 can also be used to prosecute exports or attempted exports (including the filing of false shipping documentation or license applications) that violate any U.S. law or regulation. Thus, § 554 is broader in scope than either the AECA or the EAR.

The AECA authorizes the President to "control the import and the export of defense articles and defense services." 22 U.S.C. § 2778(a)(1) (2013). Under the AECA, the President is further empowered to "designate those items which shall be considered as defense articles and defense services" and "promulgate regulations for the import and export of such articles and services." *Id.* The President has delegated this responsibility to the State Department. Exec. Order No. 11958, 42 Fed. Reg. 4311 (Jan. 18, 1977). Pursuant to its delegated authority, the State Department has promulgated the ITAR, which contains the USML. *See* 22 C.F.R. § 121.1 (2013). The USML is a list, divided into 21 categories, that identifies the types of items, services, and related technical data that are designated as defense articles and defense services under the AECA. Items or services that are designated or controlled under any category of the USML may not be exported without a license from the Department of State. 22 U.S.C. § 2778(b)(2) (2013); *see* 22 C.F.R. §§ 123.1, 127.1(a)(1) (2013). Thus, it is illegal under the AECA and the ITAR for a person to export, attempt to export, cause to be exported, or conspire to export, "any defense article, technical data, or defense service" from the United States. 22 C.F.R. §§ 127.1(a)(1)–(4) (2013).

Currently, the USML is undergoing some revisions as part of the export reform initiative "to describe more precisely the articles warranting control on the USML." See the proposed rules and amendments to the ITAR at www.pmddtc.state.gov/regulations_laws/proposed_rules.html.

While the ITAR regulates and controls the export of defense articles (including technical data) and defense services, the Department of Commerce's EAR governs the export of any item manufactured partially or entirely in the United States (and any associated technical data), except those falling under the control of another department or agency of the U.S. Government, such as the Department of State (for example, defense articles and services), the Department of Energy, or the U.S. Nuclear Regulatory Commission. *See* 15 C.F.R. § 734.3 (2013). The items falling under the control of the Department of Commerce fall into one of two categories, exclusively commercial or dual-use items. Dual-use items are those items having both a military and commercial application. *See id.* § 730.3. The EAR limits the export of goods and technology that could enhance foreign military capacities, jeopardize U.S. national security, or undermine U.S. foreign policy. The EAR places requirements on all exporters and includes a list of commodities that are subject to export controls and for which an export license may be required. *See id.* § 774.1. Whether an item requires an export license depends in part on what country the item is being exported to, who the end-user is, and what the end-user intends to do with the item.

The Commerce Control List (CCL), published within the EAR at 15 C.F.R. § 774, Supp. 1 (2013), specifies commodities, software, and technology that are subject to export controls. *See United States v. Moller-Butcher*, 560 F. Supp. 550, 552 (D. Mass. 1983); 15 C.F.R. § 774.1 (2013). In 2011, the Ninth Circuit explained that "[e]ach entry on the Commerce Control List has a particular [five character alpha-number code known as an] export control classification number [ECCN], describes the technical characteristics of the items classified with that number, and identifies the particular reasons for controlling the export of those items." *United States v. Guo*, 634 F.3d 1119, 1122 (9th Cir. 2011). The EAR also contains a second list, a Commerce Country Chart, which identifies the licensing requirements and export controls (that is, reasons for control) applied to each foreign country. *See* 15 C.F.R. §§ 738.1, 738.3, 738, Supp. 1 (2013).

There are eight different reasons items are controlled for export in the CCL, including national security, nuclear non-proliferation, anti-terrorism, and missile technology. Exports of technology controlled under the CCL are often restricted for more than one reason. Using a commodity's ECCN and

the country of ultimate destination, an exporter can determine whether a particular shipment of commodities to a specific end-user/final destination requires an export license from the Department of Commerce. *See id.* § 738.4. For instance, many of the electronic components Wu and Wei illegally exported to the PRC using Chitron-US were designated as ECCN 3A001 and were controlled for national security reasons because they had applications in military radar, electronic warfare, and missile and space systems. Because the Commerce Country Chart imposes restrictions on the PRC (but not Hong Kong) for national security reasons, these items could not be shipped to mainland China without having first obtained an export license from the Department of Commerce. *Wu*, 711 F.3d at 21–22; *accord Guo*, 634 F.3d at 1122. However, an exporter could ship these exact same goods to Hong Kong, provided the end-user is indeed located in Hong Kong, without obtaining an export license.

In addition to the ITAR and the EAR, the Department of the Treasury's Office of Foreign Assets Control also promulgates regulations to enforce economic embargos and sanctions imposed against countries that support terrorism or are involved in the proliferation of weapons of mass destruction, such as Iran. *See, e.g.*, Iranian Transactions and Sanctions Regulations, 31 C.F.R. §§ 560.204–560.211 (2013). These regulations will not be separately analyzed or discussed in this article.

B. Standard of proof in export cases

The Government's burden of proof in export cases, regardless of whether it involves a violation of the AECA and the ITAR on one hand or the EAR on the other, is very similar.

To prove an offense under the AECA and the ITAR, the Government must prove the following four elements beyond a reasonable doubt:

1. The defendant exported, attempted to export, or caused to be exported, items from the United States,
2. The items the defendant exported, attempted to export, or caused to be exported, were defense articles within the USML,
3. The defendant failed to obtain a license or other authorization from the Department of State prior to exporting the items, and
4. The defendant did so knowingly and willfully.

See Kuhali v. Reno, 266 F.3d 93, 104 (2d Cir. 2001); *United States v. Murphy*, 852 F.2d 1, 6–7 (1st Cir. 1988); 22 C.F.R. § 127.1 (2013); *see also Wu*, 711 F.3d at 18–19 (To convict defendant of violating the AECA, the jury must find that charged parts fell "within the Munitions List restrictions" at the time of the alleged illegal export.).

Similarly, to prove an illegal export under the EAR, the Government must also prove four elements:

1. The defendant exported, attempted to export, or caused the export of items from the United States,
2. The items the defendant exported, attempted to export, or caused to be exported were controlled for export on the CCL and required an export license for the destination country,
3. The defendant failed to obtain a license or other authorization from the Department of Commerce prior to exporting the items, and
4. The defendant did so knowingly and willfully.

See 50 U.S.C. § 1705 (2013); *Wu*, 711 F.3d at 21–25; *Guo*, 634 F.3d at 1123; 15 C.F.R. §§ 736.2(b)(1), 736.2(b)(10), 764.2, 764.3(b)(2)(i) (2013). To meet its burden to prove either a violation

of the ITAR or the EAR, it is critical that the Government demonstrate that the exported items were indeed subject to licensing restrictions on or before the alleged date of the illegal export.

C. Discovery issues

Prosecutors have the same discovery obligations in export cases as in other criminal prosecutions. The Government has a constitutional obligation to disclose "evidence favorable to an accused that is material to guilt or to punishment." *Cone v. Bell*, 556 U.S. 449, 451 (2009). This obligation extends to both exculpatory evidence and facts material to the impeachment of prosecution witnesses. *See United States v. Agurs*, 427 U.S. 97, 110–11 (1976).

In the discovery phase of the Chitron prosecution, the defense moved to compel the production of all documents in the Government's possession that formed the basis for the assertion that the items the defendants were accused of illegally exporting fell into the prohibited categories set forth in the regulations. This motion was denied as to the CCL controlled items, but it was granted in part with regard to the AECA counts. The court ordered the Government to produce any documents in its possession "that could significantly refute the Government's case in chief . . . on the issue of willfulness." *United States v. Wu*, 680 F. Supp. 2d 287, 290 (D. Mass. 2010). Consequently, "if either the Department of State's or the Department of Commerce's files have any evidence that tends to support a defense of lack of willfulness (that is, a manufacturer's indications that the articles allegedly exported have normal commercial uses) such information must be produced." *Id.* at 291.

In the typical AECA prosecution, it is unlikely that the Government will have many documents related to a specific manufactured defense article, other than the Department of State's pre-trial certification and/or trial certification that confirms for the prosecutor and the court that a certain product is a defense article designated on the USML. If, however, the parts at issue were subject to a commodity jurisdiction (CJ) determination or government jurisdiction (GJ) determination process, there may be internal documents or files at the Department of State that contain discoverable information. For instance, three of the six defense articles Wu, Wei, and Chitron-US were charged with illegally exporting in the substantive AECA counts had been the subject of a CJ or GJ determination.

The CJ or GJ determination procedure can be used by anyone (albeit it is typically requested by the manufacturer) to determine whether a specific item or service is covered by the USML. *See* 22 C.F.R. § 120.4 (2013). It is the exporter's obligation to obtain any necessary export licenses prior to shipping any U.S. commodity outside the United States. Thus, if an exporter cannot determine whether a certain commodity is a defense article designated on the USML, the exporter can submit a commodity jurisdiction request, pursuant to 22 C.F.R. § 120.4, to the Department of State's Directorate of Defense Trade Controls (DDTC). Manufacturers may use this same procedure if they have doubt as to whether any of their products are covered by the USML or if they would like DDTC to consider re-designating one of their products or services. (Similarly, if an exporter cannot determine the ECCN for a product it is exporting, the exporter can submit a commodity classification request to the Department of Commerce.) Occasionally, the Government itself may initiate a jurisdiction review (that is, an evaluation of whether a product falls under the jurisdiction of the Department of State or the Department of Commerce) of a product. When this process is initiated by a government official rather than a private party, it is referred to as a GJ determination.

During the CJ/GJ process, DDTC consults with, and requests information from, the Departments of Defense and Commerce, in addition to any agency with specialized knowledge of the part at issue (for example, NASA, Army, Navy, Air Force, etc.). *See* 22 C.F.R. § 120.4(a) (2013). Occasionally, the government agencies come to different conclusions as to whether a part is covered under the USML. For instance, with regard to one of the parts Chitron-US was charged with illegally exporting to China, the M/A-Com 6-bit MAPCGM0003 phase shifter—which according to the manufacturer was used primarily in military phased array radar and had no known commercial uses—Department of Commerce officials

concluded that these phase shifters fell within its jurisdiction, were used in numerous civil applications, and should be classified as "EAR99," meaning no export license would be required to ship it to most countries. *See* Defense Exhibit 7. In direct contrast, the Department of Defense concluded that these phase shifters constituted critical military technology and "must be protected in the interest of national security." Government Exhibit 613. Furthermore, the Defense Technology Security Administration advised the DDTC that the MAPCGM0003 phase shifters were

> designed for use in military phase array radar applications, and could also be used for military satellite communications and Electronic Warfare (EW). As a result, it could be used in the development of advanced AESA radar or an Electronic Attack (EA) system, which could significantly impair US military operations in the region.

Id.

These different conclusions may arise from the strikingly different purposes of the agencies from which the Department of State seeks the information. Unlike the Department of Defense, whose mission is to protect national security and safeguard critical military technology, the Department of Commerce's objective is to promote trade. It is therefore not surprising that Department of Commerce officials often try to persuade the Department of State that items have primarily civilian or commercial applications and should be regulated under the CCL, thereby reducing the export license requirements and allowing trade with countries like the PRC that otherwise would be prohibited under the U.S. Arms Embargo.

Regardless of who weighs in, the final decision during the CJ process as to whether a part "is covered by the U.S. Munitions List" is made by the State Department's DDTC. *See* 22 C.F.R. § 120.4(a) (2013). Recently, DDTC has begun publishing these CJ decisions on its Web site. Currently, CJ determinations issued from 2010 through 2012 are available. *See* COMMODITY JURISDICTION FINAL DETERMINATIONS, www.pmddtc.state.gov/commodity_jurisdiction/determination.html. Like the CJ determinations, USML "designations are made by the Department of State with the concurrence of the Department of Defense." 22 C.F.R. § 120.2 (2013).

D. Typical defense motions

In historical investigations like Chitron, defendants have challenged the AECA on due process grounds. Like many other defendants, Wu and Wei moved to dismiss the AECA counts on the ground that the AECA and the ITAR are unconstitutionally vague and failed to provide them sufficient notice that the charged conduct was illegal. At least five circuit courts of appeal have rejected constitutional challenges to the AECA.

"The Fifth Amendment's Due Process Clause requires that 'a criminal statute provide adequate notice to a person of ordinary intelligence that his contemplated conduct is illegal.' " *Wu*, 711 F.3d at 13 (quoting *Buckley v. Valeo*, 424 U.S. 1, 77 (1976) (per curiam)). Under the void-for-vagueness doctrine, a statute or regulation that criminalizes conduct must (1) "define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited" and (2) be executed "in a manner that does not encourage arbitrary and discriminatory enforcement." *Kolender v. Lawson*, 461 U.S. 352, 357 (1983). "But 'where, as here, a criminal statute regulates economic activity, it generally is subject to a less strict vagueness test.' " *United States v. Hsu*, 364 F.3d 192, 196 (4th Cir. 2004) (quoting *United States v. Sun*, 278 F.3d 302, 309 (4th Cir. 2002)).

Economic regulation is "subject to a less strict vagueness test because its subject matter is often more narrow, and because businesses, which face economic demands to plan behavior carefully, can be expected to consult relevant legislation in advance of action." *Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498 (1982); *accord United States v. Lee*, 183 F.3d 1029, 1032 (9th Cir. 1999); *see United States v. Lachman*, 387 F.3d 42, 56–57 (1st Cir. 2004) (The fact that export laws require interpretation does not render them unconstitutionally vague as they are addressed to sophisticated

businessmen and corporations, which can "consult counsel in planning their activities, and where an administrative process exists to secure advisory interpretations of the statute."). Also, "the regulated enterprise may have the ability to clarify the meaning of the regulation by its own inquiry, or by resort to an administrative process." *Hoffman Estates*, 455 U.S. at 498. In any event, "a scienter requirement may mitigate a law's vagueness, especially with respect to the adequacy of notice to the complainant that his conduct is proscribed." *Id.* at 499; *accord United States v. Hescorp, Heavy Equip. Sales Corp.*, 801 F.2d 70, 77 (2d Cir. 1986) (rejecting defendant's vagueness challenge to Iranian Embargo Regulations, noting that "a requirement of willfulness makes a vagueness challenge especially difficult to sustain"); *Lee*, 183 F.3d at 1033 ("[I]nclusion of a scienter requirement significantly reduces any concern that the statute and regulation fail to provide proper notice.").

Applying these standards, courts have repeatedly rejected vagueness challenges to the AECA and USML. *See Wu*, 711 F.3d at 14–16 (rejecting vagueness challenge to the AECA and its implementing regulations); *Hsu*, 364 F.3d at 196–97 (same); *Sun*, 278 F.3d at 309–10 (same); *Lee*, 183 F.3d at 1032–33 (same); *United States v. Gregg*, 829 F.2d 1430, 1437 (8th Cir. 1987) (same); *United States v. Swarovski*, 592 F.2d 131, 133–34 (2d Cir. 1979) (rejecting vagueness challenge to the AECA's predecessor statute). Courts have cited three principal reasons in rejecting vagueness challenges to the AECA. First, a less strict vagueness test applies because the AECA regulates a narrow economic activity—the exportation of military equipment—managed by "a relatively small group of sophisticated international businessmen." *Lee*, 183 F.3d at 1032. Second, anyone who is unsure whether a particular commodity is covered by the USML can resolve the perceived ambiguity by asking the DDTC, a fact which mitigates any purported vagueness. *Wu*, 711 F.3d at 15; *see* 22 C.F.R. § 120.4 (2013); *see also Lee*, 183 F.3d at 1032 (The ability to "contact the appropriate government agency to resolve any perceived ambiguity" mitigates any vagueness.). Third, and perhaps most important, the AECA has a scienter requirement: A defendant can only be held criminally responsible for "willfully" exporting defense articles without a license. 22 U.S.C. § 2778(c) (2013); *Lee*, 183 F.3d at 1032–33. This willfulness requirement makes a vagueness challenge especially difficult, as "[a] mind intent upon willful evasion is inconsistent with surprised innocence." *United States v. Ragen*, 314 U.S. 513, 524 (1942); *see Hsu*, 364 F.3d at 197 n.1 (explaining that "requiring the jury to find a defendant acted 'willfully' necessarily leaves 'innocent' exporters outside the statute's scope and so vitiates any vagueness concerns"); *Lee*, 183 F.3d at 1032–33 (holding that AECA's scienter requirement "protects the innocent exporter who might accidently and unknowingly export a proscribed component or part whose military use might not be apparent through physical appearance"); *see also Swarovski*, 592 F.2d at 132 (stating that a vagueness challenge "comes with little grace from one who was fully cognizant of the wrongfulness of his acts").

In rejecting Wu and Wei's vagueness arguments, the First Circuit noted that "it is not too much to ask these businessmen and businesswomen [who run international operations involving the export of military equipment] to comply with export control regulations, even if the meaning of those regulations might not be immediately obvious to someone lacking the same sophistication." *Wu*, 711 F.3d at 14. Further, the court concluded that "Wu and Wei repeatedly attempted to disguise the fact that they were exporting to China and that they lacked the necessary licenses to do so." *Id.* at 16. This evidence demonstrated that the defendants "knew they were violating U.S. export regulations," which refuted the defendants' claims that "they lacked 'fair notice' of the [ITAR's] Category XI(c) restrictions." *Id.*

Additionally, courts have also rejected vagueness challenges to the other U.S. export laws, including the EAR. *See United States v. Guo*, 634 F.3d 1119, 1122–23 (9th Cir. 2011) (The EAR satisfies due process because they "apprise those who take the time and effort to consult them as to what may and may not be taken to other countries without a license and do not allow for arbitrary enforcement."); *United States v. Quinn*, 401 F. Supp. 2d 80, 100–01 (D.D.C. 2005) (denying defendant's due process challenge to Iranian Transaction Regulations, which prohibit exports to Iran, and concluding that the Iran trade embargo laws "are not apt to sweep within their coverage the everyday acts of average citizens. Rather, they govern the activities of relatively sophisticated individuals who are deliberately engaged in

international commerce and, therefore, must be familiar with (if not expert in) various legal regimes—e.g., customs duties and tariffs—in multiple countries.").

E. Trial

Proving the willfulness element: Typically, the defense's primary attack at trial in export cases involves the element of willfulness. The defendant often argues that he did not know that his conduct was unlawful.

> In order to prove that the defendants acted willfully, the
>
> government must show that a defendant knew that the exportation of . . . [the item] was illegal [however], it is not necessary for the government to show that the defendants were aware of or had consulted the United States Munitions List or the licensing and registration provisions of the Arms Export Control Act and its regulations.

United States v. Murphy, 852 F.2d 1, 7 (1st Cir. 1988). *Murphy* is consistent with *Bryan v. United States*, 524 U.S. 184 (1998), in which the Supreme Court held that to prove that a defendant "willfully" dealt in firearms without a federal license, the Government must prove only the defendant's "knowledge that the conduct is unlawful," not knowledge of the specific licensing requirement he violated. *Bryan*, 524 U.S. at 196, 199. Every other circuit to address this issue in the export context has held similarly. *See United States v. Mousavi*, 604 F.3d 1084, 1093–94 (9th Cir. 2010) (relying upon *Bryan* in rejecting defendant's argument that Government was required to prove defendant "had a specific understanding of the [Iranian Transaction Regulations'] licensing requirements" to sustain conviction under IEEPA and finding it sufficient for Government to prove defendant "knew he was acting unlawfully"); *United States v. Piquet*, 2010 WL 1267162, at *3 (11th Cir. Apr. 5, 2010) (concluding that the Government is not required to prove defendant read, was aware of, or consulted the USML or the CCL to establish willful violation of the AECA or EAR); *United States v. Elashyi*, 554 F.3d 480, 505 (5th Cir. 2008) (adopting *Bryan* standard for willfulness in an IEEPA case and approving district court's instruction to jury that "willfully" means "with the specific intent to do something the law forbids; that is to say, with the bad purpose either to disobey or disregard the law"); *United States v. Brodie*, 403 F.3d 123, 146–47 (3d Cir. 2005) (in a Trading With the Enemy Act case, required showing only that defendant knew export was unlawful); *United States v. Homa Int'l Trading Corp.*, 387 F.3d 144, 146–47 (2d Cir. 2004) (approving jury instruction requiring showing only that defendant knew actions, which involved transferring funds to Iran, were illegal); *Hsu*, 364 F.3d at 198 n.2 (citing *Murphy* and stating that "[w]hatever specificity on 'willfulness' is required, it is clear that [an] extremely particularized definition finds no support in the case law"); *United States v. Huynh*, 246 F.3d 734, 742 (5th Cir. 2001) (in Trading With the Enemy Act prosecution, "government . . . need not show that [defendants] had knowledge of the specific regulations governing [their conduct] . . . [but r]ather . . . must prove only that the defendants knew that their planned conduct was legally prohibited"); *United States v. Tsai*, 954 F.2d 155, 162 (3d Cir. 1992) (in an AECA case, approved jury instruction requiring showing only that defendant knew the export was illegal). Most recently, the Sixth Circuit held that "section 2778(c) does not require a defendant to know that the items being exported are on the USML. Rather, it only requires knowledge that the underlying action is unlawful." *United States v. Roth*, 628 F.3d 827, 835 (6th Cir. 2011); *accord United States v. Chi Mak*, 683 F.3d 1126, 1137–38 (9th Cir. 2012) (finding no error in jury instructions for the AECA offense that equated willfulness element with proof that defendant violated "a known legal duty" and specifically stating that Government was "not required to prove that 'the defendant had read, was aware of, or had consulted the specific regulations governing his activities' ").

In dicta in *United States v. Pulungan*, 569 F.3d 326 (7th Cir. 2009), the Seventh Circuit seemed to suggest that the Government might be held to a higher burden in future prosecutions but fell short of reversing the controlling authority in that circuit, which is consistent with *Murphy*. The *Pulungan* court stated:

> Pulungan cannot be convicted unless he *knew* that [a Leupold Mark 4 CQ/T riflescope] is [a "defense article"], and that licenses are necessary to export them. The United States concedes that the word "willfully" in § 2778(c) requires it to prove that the defendant knew not only the material facts but also the legal rules. (We need not decide whether the concession is correct. "Willfully" is a notoriously plastic word. *See Bryan v. United States*, 524 U.S. 184 (1998)).

Pulungan, 569 F.3d at 329 (emphasis in original). But, as the *Pulungan* court noted, the Government had conceded the heightened definition of willfulness, so the court therefore did not decide whether this definition was correct. In light of this, as well as controlling Seventh Circuit precedent, such as *United States v. Beck*, 615 F.2d 441, 450–51 (7th Cir. 1980) (requiring Government to show only that defendant knew his conduct was illegal, not that the defendant knew of need for export license pursuant to the AECA), a claim that the *Pulungan* court changed the definition of "willfully" in the AECA context to require proof of knowledge of the licensing requirement, as opposed to proof that the defendant knew that his actions violated a legal duty, is unlikely to succeed.

Proving charged parts constitute defense articles controlled under USML: In *Wu*, the First Circuit explained that whether or not a specific item falls within a category on the USML is a factual question for the jury unless the State Department has made the designation determination prior to "the time that the defendants engaged in the charged conduct." *Wu*, 711 F.3d at 18–20. While the First Circuit did not clarify how the State Department must make such an official pre-offense designation (that is, publicly in the ITAR, on its Web site, or privately in the form of a certification for investigators or prosecutors), if any document exists, it would likely be admissible and assist the Government in meeting its burden. To prove that parts constitute defense articles, prosecutors should consider calling technical experts who were involved in the development of the charged item or technical data, Government technical experts (military engineers or scientists employed within the Defense Technology Security Administration), as well as officials from DDTC who could render their legal opinion that the charged item, technical data, or service falls under a certain category of the USML.

As this article is being drafted, the ITAR is being amended as part of the Export Control Reform initiative. Each category of the USML has been or is in the process of being reviewed and amended to "create a more positive control list and eliminate where possible 'catch all' controls." *See, e.g.*, Amendment to the International Traffic in Arms Regulations: Continued Implementation of Export Control Reform, 78 Fed. Reg. 40,922, 40,922 (July 8, 2013). These changes may eliminate the need for prosecutors to "prov[e] anew each time" that the charged part was indeed "within the scope of the Munitions List." *See Wu*, 711 F.3d at 20 n.11 (Proposed amendments to USML Category XI "specifically" includes phase shifters and, therefore, "if finalized, it would permit the government to prosecute future exporters without proving anew each time that phase shifters are within the scope of the Munitions List.").

CCL export and license exception issues: Unlike the USML, license exceptions are available to certain categories of the CCL, and not every export requires a license. Accordingly, at trial, the defendant may attempt to assert that a license exception applied and his conduct therefore did not violate the EAR. This defense can be greatly undermined if you can show that the exporter falsified the shipping documentation. Typically, to avail oneself of a license exception within the EAR, an exporter must correctly classify the exported item and list any applicable license exceptions on the Shipper's Export Declaration at the time of the export. Merely listing the acronym "NLR" (no license required) rather than the ECCN, does not suffice.

As explained above, many of the electronic components Wu and Wei illegally exported to the PRC using Chitron-US were controlled under ECCN 3A001. While these parts required an export license to ship them to the PRC, they did not require a license to go to Hong Kong. Thus, the Government was required to show the parts were ultimately shipped to mainland China; it was not sufficient to prove that

they went to a freight forwarder in Hong Kong. Further, during trial, Wu and Wei claimed that a license exception, the Additional Permissive Re-export (APR) Exception, *see* 15 C.F.R. § 740.16, applied to their conduct and that they were therefore relieved of any obligation to obtain export licenses for the electronic components controlled under the ECCN 3A001. The APR exception allows U.S. commodities that have been exported to Hong Kong to be re-exported to China without obtaining a re-export license from the United States. However, if the exporter had the knowledge at the time of the original export from the United States that the final destination for the commodities was China (not Hong Kong), a license is required and this exception does not apply.

We defeated this defense by showing that the parts were never intended to stay in Hong Kong (that is, they never entered the stream of commerce or were to be treated as inventory). To the contrary, the parts had been ordered and purchased for specific customers located in mainland China and within days of arriving at the freight forwarder's office in Hong Kong were delivered to Chitron-Shenzhen's warehouse.

To overcome the APR exception or a similar defense, prosecutors should introduce as many documents as possible about the end-user of the illegally exported item(s). Such documents will often demonstrate the actual location of the end-user rather than the freight-forwarder or intermediate consignee, the end-use for the parts sought (military versus commercial), and the date the end-user ordered or requested the items from the exporter/distributor (for example, U.S. origin goods obtained for certain customer and not for inventory so APR exception not applicable). This evidence may prove critical to establishing that the alleged export was, indeed, illegal and a knowing and willful violation of the EAR.

IV. Sentencing

A. Sentencing guidelines

Currently, the United States Sentencing Guidelines (U.S.S.G.) do not distinguish between cases involving the export of a single item or those involving hundreds of parts over a long period of time. The base offense level (BOL) is 26 for a single export of either (1) commerce export restricted parts controlled for national security reasons (ECCN 3A001) or for nuclear proliferation reasons, or (2) items designated on the USML. *See* U.S. SENTENCING GUIDELINES MANUAL §§ 2M5.1, 2M5.2 (2012). Thus, the BOL that applied to both defendants, Wu and Wei, was 26, which assumed that the defendants were only convicted of one illegal export when in fact the defendants were convicted of conspiring to illegally export and illegally exporting hundreds of electronic components to the PRC. The notes to §§ 2M5.1 and 2M5.2 indicate that an upward departure from the Guidelines may be warranted where, like here, the conduct was egregious, involving numerous violations, hundreds of parts, and extensive planning, which seriously threatened national security. Many judges, however, are uncomfortable upwardly departing. Thus, it would be preferable to have a graduated scale that would increase the offense level based on either the number of exports or the value of the exports. *See, e.g.*, U.S. SENTENCING GUIDELINES MANUAL § 2K2.1(b)(1) (2012) (number of firearms triggers increase in BOL).

B. Present evidence that defendant's conduct threatened national security

Because the U.S.S.G. is merely advisory, it is incumbent on the prosecutor to educate the bench about the national security implications of the defendant's illegal export activities or attempted activities to ensure that the defendant gets an appropriate sentence. Further, defense counsel could attempt to persuade the court that a downward departure is warranted. *See* U.S. SENTENCING GUIDELINES MANUAL § 2M5.2, app. 1 (2012) ("The base offense level assumes that the offense conduct was harmful or had the potential to be harmful to a security or foreign policy interest of the United States. In the unusual case where the offense conduct posed no such risk, a downward departure may be warranted."). At the

sentencing hearings of defendants Wu and Wei, we submitted a report from the Director of the Defense Technology Security Administration, Office of the Secretary of Defense for Policy, Department of Defense (DTSA). In this report, DTSA concluded that the defendants' activities seriously threatened "U.S. national and regional security interests" and that the parts the defendants were convicted of illegally exporting are "vital for Chinese military electronic warfare, military radar, fire control, military guidance and control equipment, and satellite communications." Exhibit A to Government Memorandum (Jan. 20, 2011). DTSA went on to state that the charged parts are "precisely the [types of] items . . . that the People's Liberation Army actively seeks to acquire" as part of its military modernization effort. According to DTSA's report, the PRC's modernization effort "has become a serious national issue for the U.S." *See id.*

C. The importance of deterrence

Even if local media is not interested in your case, the foreign media likely is. It quickly came to our attention that the Chinese media outlets had far more interest in the prosecution of Chitron, Wu, and Wei than the Massachusetts newspapers or any national media agencies. Indeed, Chinese reporters attended several days of the trial. We brought this to our judge's attention during sentencing. In addition, we specifically argued general deterrence during the sentencing hearings. During the sentencing of Wu, the judge indicated that she was imposing a sentence of 84 months' imprisonment because of the significant national security concerns and to deter others from similarly violating U.S. export laws.❖

ABOUT THE AUTHOR

❑**B. Stephanie Siegmann** is an Assistant U.S. Attorney assigned to the Anti-Terrorism and National Security Unit of the U.S. Attorney's Office for the District of Massachusetts. She investigates and prosecutes matters involving international terrorism, domestic terrorism, espionage, misuse of classified information, and export violations. Since 2007, Ms. Siegmann has served as the Export Case Coordinator and Chair of the Massachusetts Counter-Proliferation Working Group (CPWG), which consists of representatives of law enforcement intelligence agencies. The CPWG shares information regarding current threats and suspicious activities regarding the transfer of sensitive U.S. technology through illegal means and coordinates investigations. Prior to joining the U.S. Attorney's Office in 2003, Ms. Siegmann worked as a litigation associate at Edwards & Angell, LLP and Hill & Barlow, PC. Prior to working in private practice, Ms. Siegmann served as trial counsel in the Navy Judge Advocate Corps. She resigned her commission as a Navy Lieutenant after prosecuting numerous cases involving crimes such as murder, rape, computer crimes, fraud, child abuse, and drug offenses.✠

Challenges and Lessons Learned in IEEPA Counter-Proliferation Cases: *United States* v. *Susan Yip*

Mark Roomberg
Assistant United States Attorney
National Security Coordinator
Western District of Texas

This article will discuss challenges and lessons learned both generally as well as in the context of a counter-proliferation case we did in the Western District of Texas. As with all successful cases, the key in counter-proliferation cases is to have a good team of agents and prosecutors. I am a firm believer that each agency brings its own expertise and resources to the table. In San Antonio, we are fortunate to have agencies that work well together. That being said, not all districts have agencies that "play nice" together. A way to facilitate agency collegiality, whether or not you are in a district where the agencies get along, is to set up a Counter-Proliferation Task Force. In 2007, the Assistant Attorney General (AAG) of the National Security Division (NSD) began an export enforcement initiative, starting with the formation of Counter-Proliferation Task Forces based in each district, that would be led by the U.S. Attorney's office. Having the prosecutor lead the task force connects and alleviates many of the interagency issues that might be present. Because counter-proliferation cases, by their very nature, involve countries and people that give rise to national security issues and intelligence collection, I would highly recommend that you have at least one agency that is part of the intelligence community (IC), such as the FBI, in order to help navigate through these sensitive issues. My last general recommendation is that as soon as you open a counter-proliferation case file, make contact with the NSD's Counterespionage Section (CES) to assign an attorney. The assigned attorney can assist you to get NSD prosecution approvals, make a prudential search request for *Brady* material to the IC, help coordinate with the Criminal Division's Office of International Affairs for lures, and generally gain CES's expertise and experience.

Prior to the 2007 AAG memorandum, our counter-proliferation group consisted of the FBI, Immigration and Customs Enforcement (ICE), now Homeland Security Investigations (HSI), and the Defense Criminal Investigative Service (DCIS). After the AAG memorandum came down in 2007, the Commerce Department's Bureau of Industry and Security (BIS) joined our task force. In terms of division of labor, while all the agencies would jointly work the cases, the agencies agreed that the FBI would focus on the national security intelligence angle while ICE, BIS, and DCIS would primarily focus on making the criminal cases. Our DCIS agent had recently come from their Boston office, where they had done some great cases, and he brought a great deal of experience to the table.

The first test of our task force came with the June 2008 case opening on Susan Yip, a/k/a Susan Yeh, a Taiwanese national living in both Taiwan and Hong Kong. Yip came to ICE and BIS's attention when she attempted to purchase parts from a company in the Western District of Texas (WDTX). Email search warrants yielded a wealth of information. The emails showed that Yip was the broker and conduit for an Iranian national living in Tehran. The Iranian national would instruct Yip which parts he wanted her to purchase from the United States and ship to him in Iran. Yip would inform the companies directly, or through brokers, that the ultimate end-user was either in Taiwan or Hong Kong because there was no prohibition on sending these particular items to these two countries if that was where the true ultimate end-user was located. Yip and the Iranian national would communicate with each other via email about their scheme and plans and the progress of the purchases and shipments to Iran. After purchasing the

goods and items from the United States on behalf of the Iranian national, Yip would then ship the items to him or transship the goods through a freight forwarder in the United Arab Emirates (UAE), who would then forward the goods to the Iranian national. From Iran, the Iranian national would cause bank wire transfers to issue to pay Yip and the UAE freight forwarder. Using the funds sent by the Iranian national from Iran, Yip would pay the United States companies supplying the goods. Obviously, given the final destination of the goods, none of the conspirators attempted to get the proper export license.

One of the first hurdles we encountered in this case was sorting through the enormous volume of emails because Yip was such a prolific procurer of U.S. goods. The ICE and DCIS agents took the primary responsibility of sorting through 300,000 emails and narrowing it down to about 2,000 for my review to determine which would be trial exhibits and overt acts evidence for the indictment. In the end, the volume of emails was both a curse in terms of the sheer time it took to review and a blessing in the wealth of evidence it produced.

A common problem in counter-proliferation cases is proving the element of willfulness, that is, that the defendant knew their conduct in sending U.S. products to Iran was unlawful. Because of the volume of the emails and the candid nature of Yip and the Iranian national's conversations, the willfulness element did not present a problem in this case. Yip and the Iranian national openly discussed the illegality of purchasing U.S. goods and parts to send to Iran, as Iran was an embargoed country. Another way the agents nailed down the willfulness element was having BIS reach out to Yip after the agent stopped the shipment of the WDTX goods before it left the country. The BIS agent then took on the role of trying to "help" Yip get the goods coming from the WDTX and communicated with her via email. Through this email communication, the BIS agent clearly put her on notice as to the export laws and explained the necessity of being truthful about the actual end-user. When all was said and done, Yip continually lied to the BIS agent as to the ultimate end-user. However, we had her emails to the Iranian national and the UAE freight forwarder discussing the need to avoid letting the U.S. freight forwarder know the goods were going to Iran. These multiple communications between the BIS agent and Yip also allowed us to shore up our venue for our conspiracy charge because we had only one shipment from the WDTX and hundreds of others from the United States and around the world.

The next issue to confront, as is common in both counter-proliferation and cyber intrusion cases, was our need to prove that Yip was actually the one behind the computer keyboard ordering all of these parts for Iran, as opposed to someone just using her name. To solve this issue, BIS and ICE arranged an overseas inspection of Yip's purported end-use location in order to identify her face-to-face and get a copy of her ID.

Our next complication was the extreme difficulty of determining what each ordered part was used for, because of the sheer volume of goods and parts that Yip tried to get for the Iranian national. In our case, the defendants obtained, or attempted to obtain, from companies worldwide 105,992 parts valued at approximately $2,630,797.53 and involving 1,261 transactions. The defendants conducted 599 transactions with 63 different U.S. companies where they obtained, or attempted to obtain, parts from U.S. companies without notifying those companies that these parts were being shipped to Iran or attempting to get the proper export licenses to ship the parts to Iran. With very few exceptions for humanitarian or religious items, sending any U.S. goods to Iran or other embargoed countries is illegal.

To make a stronger case for the jury and to make sure the sentencing judge would give at least a guideline sentence, we wanted to explain what the uses were of the parts the Iranian national was ordering. In cases where you have one, two, or just a few parts, the easy solution is to call a witness or witnesses from the parts' producer and ask them about the parts' potential uses. Because we had so many parts, this approach was not feasible. Moreover, many of the agencies that have access to such expertise were not willing to let their experts testify despite numerous requests from our ICE, BIS, and DCIS agents. In the end, our FBI agent tracked down an expert witness from the Sandia Lab who was on temporary duty with the FBI in Washington. After reviewing the parts, our expert determined that while

individually these parts had dual-use military and civilian capability, when viewing Yip and the Iranian national's shopping list as a whole, the expert opined that they were buying these parts to use in such systems as nuclear weapons, missile guidance and development, secure tactical radio communications, offensive electronic warfare, military electronic countermeasures (radio jamming), and radar warning and surveillance systems.

Once we had an expert witness, we needed to decide on what charges to bring and how the charges would impact possible extradition scenarios. I decided to lead off with a conspiracy to violate the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1705, and the Iranian Transaction Regulations (ITR), 31 C.F.R. § 560. This charge allowed me to explain the law and lay out the entire scheme without any Federal Rule of Evidence 404(b) issues. As I said previously, except for the one purchase from the WDTX that included numerous telephone and email contacts between Yip and both the company and the BIS agent, the other 598 U.S. transactions occurred outside our district. I have found this type of venue scenario is more common than not in counter-proliferation cases.

One of the biggest problems in counter-proliferation cases is that after all the hard work of putting the case together and taking it to the grand jury is done, you still have to lay hands on the target. While we have extradition treaties with many countries around the world, frustratingly, very few if any of them will extradite targets to the United States based on IEEPA and ITR charges. With that in mind, I decided to also charge conspiracy to commit wire fraud in violation of 18 U.S.C. §§ 371, 1343, conspiracy to commit money laundering in violation of 18 U.S.C. § 1956(h), conspiracy to defraud the United States in violation of 18 U.S.C. § 371, and making false statements in violation of 18 U.S.C. § 1001. These non-IEEPA/ITR charges are covered by the vast majority of the extradition treaties, either under the listed offenses or the "dual criminality" clauses, which allows the countries to extradite to the United States if a particular country where the defendant was captured would not extradite for IEEPA/ITR crimes.

It is said that "patience is a virtue." This statement is especially true in cases involving defendants who do not travel to the United States. Because of the defendant's lack of travel to this country, it took three years working with CES and OIA to come up with a viable lure plan that would allow for a successful prosecution without the chance of an extradition attempt falling through. After receiving lure approval from OIA in 2011, we attempted to lure Yip to a U.S. territory in the Pacific in 2011. Unfortunately, the defendant got cold feet a week before the trip and cancelled. Because of some brilliant undercover work by one of our HSI agents pretending to be a contractor seeking Yip's services in a legitimate LED lighting business that Yip ran, the agent got Yip to come to San Antonio in the summer of 2012 to train the agent's fictional employees on how to install the lighting that the agent "wanted to buy" from Yip. After four years of investigating this case and three years of building the relationship between the undercover agent and Yip, Yip landed in Los Angeles.

We had decided that we wanted Yip well rested when we debriefed her. Therefore, we did not want to have her arrested as soon as she landed in the United States so that we could bring her to San Antonio to have one final conversation with the undercover agent and allow her to verbally implicate herself about how she was willingly helping the Iranians get these U.S. goods. The agent met with Yip on that day and took her out to dinner. All of the agencies shared the surveillance duties that afternoon and evening. The takedown occurred at the undercover agent's lighting "office," which was in fact the HSI/DCIS office (without the signs, of course), after the undercover agent brought Yip there. The FBI provided the Mandarin interpreters that made for a successful debriefing.

Because of ongoing operations, it was decided ahead of time that we would seek Deputy Attorney General authorization to seal the courtroom. Once we knew Yip had arrived in San Antonio, we notified the magistrate judge that we would be arresting a defendant the next day. Because we knew we would be seeking the defendant's cooperation, we asked the magistrate to have an interpreter available and to request a defense attorney to be on stand-by for the initial appearance. The courtroom remained sealed for

the eventual guilty plea and was not unsealed until Yip's sentencing, when the operational phase was complete. Yip was sentenced to two years in custody.

A final word of caution, if you believe it is necessary to actually ship a product to an embargoed country in order to make your case, you will need "Otherwise Illegal Activity" approval and an undercover Office of Foreign Assets Control license. One of your case agents will need to file this request through his or her headquarters, along with possibly needing to get the blessings of other agencies. This is one of the many times you will be glad to have brought in CES early and have one of their attorneys help you navigate this delicate area.

As I said in the beginning, successful prosecutions are a team effort, especially in the counter-proliferation realm. From the prosecution angle, I could not have done this without the help of CES. A now former Assistant U.S. Attorney from Miami was kind enough to both send her indictments as well as clue me in on debarments. I always believed that it was better to keep indictments sealed as to all fugitive defendants rather than make a press splash. This strategy is a good one when extradition is a viable option. However, when extradition and lures are not viable options and never will be, debarments can put some real obstacles to individuals trying to obtain U.S. goods in violation of the law, and sometimes the "name and shame" option is the only one available. Besides the unique skill set that our task force agents had, they could not have been as successful without the assistance of their headquarter components, insights from other squads around the country, and the overseas components of these agencies. I am only too happy to give back what was so freely given to me. If you have a counter-proliferation case and would like indictment samples or professional memo go-bies, or just want to bounce ideas around, please feel free to send me an email on DOJ Outlook.❖

ABOUT THE AUTHOR

❑**Mark Roomberg** has been with the U.S. Attorney's Office for Western District of Texas for 19 years and was at the Tax Division, Criminal Enforcement Section for 5 years prior. He has been serving as the district's National Security and ATAC Coordinator for seven years and is currently serving as the chief of the San Antonio Division's White Collar and Public Corruption Unit. ✠

Establishing the Lack of a License: More Than an Afterthought

Jay Bratt
Deputy Chief
National Security Section
District of Columbia

I. Introduction

Your export case is nearing its end. You have introduced the emails in which the defendants openly scheme to evade U.S. export controls on a variety of widgets necessary for the construction of a nuclear warhead. You have introduced the tapes of the undercover meetings at which the defendants joke

about supplying crucial military aircraft components to a hostile regime. The evidence of willfulness is overwhelming, and there is nothing else left to do but to go to closings and then await the verdict.

But wait—your case is not over yet. You need to call a licensing official from the appropriate regulatory agency to demonstrate that the defendants needed a license and never obtained one for their otherwise unlawful export. Taking this step is necessary because the failure to get a license is an element of every type of export violation. *E.g.*, *United States v. Murphy*, 852 F.2d 1, 6 (1st Cir. 1988) (violation of the Arms Export Control Act (AECA) and the State Department's International Traffic in Arms Regulations (ITAR)); *United States v. Gregg*, 829 F.2d 1430, 1435–36 (8th Cir. 1987) (violation of the International Emergency Economic Powers Act (IEEPA) and the Department of Commerce's Export Administration Regulations (EAR)); *United States v. Quinn*, 403 F. Supp. 2d 57, 63 n.4 (D.D.C. 2005) (violation of IEEPA and the Iranian Transaction Regulations administered by the Department of the Treasury's Office of Foreign Assets Control (OFAC); court suggests that the licensing provision may create an affirmative defense rather than serve as an element of the offense, but accepts the Government's charging decision to treat failure to obtain a license as an element of the crime).

This article examines some of the issues that can arise when prosecutors seek to introduce evidence to satisfy the Government's burden of proving that a particular commodity required a license for export to its ultimate destination. In general, the ease of proving this element will vary depending on the export regime in question. For the sanctions regimes administered by the Department of the Treasury and OFAC, the proof will be relatively simple. A single witness will be able to testify as to the need for a license and the defendant's lack of the appropriate approval. However, in light of some recent cases, establishing that a commodity is subject to the ITAR, and therefore needs a license, can be more complicated. Depending on the item, this situation may require the Government to call both an expert on the product and a representative from the State Department to testify. With respect to items under the purview of the Department of Commerce, the level of difficulty is somewhere in the middle.

This article also examines some suggested topics to cover with the licensing witnesses. While the subject matter of their testimony may seem dry, it is possible to use these witnesses as an additional means of strengthening your cases. Some suggested questions are set forth in section IV at the end of this article.

II. How to establish the need for and absence of a license

A. Cases charging violations of the AECA and the ITAR

Section 121.1 of the ITAR is known as the Munitions List, and it contains broad categories of commodities that are "defense articles." *See* 22 C.F.R. § 121.1 (2013). For many years, it was the State Department's position, consistent with court rulings, that whether a particular item was a defense article subject to the ITAR was not a matter for judicial review or for the jury to decide. *See Karn v. Dep't of State*, 925 F. Supp. 1, 4–8 (D.D.C. 1996). *See also* 22 U.S.C. § 2778(h) (2013) (Designation by the President of items as defense articles shall not be subject to judicial review). Thus, at trial, it was only necessary to call someone from the State Department's Directorate of Defense Trade Controls (DDTC), which administers the ITAR, to testify that the commodity in question was a defense article and that the defendants never obtained a license to export it. However, two cases in recent years from the Seventh and First Circuits have rejected such an approach and reversed the AECA convictions. Instead, these cases held that whether an item was a defense article was a matter for the jury to determine and that the Government must introduce proof to support such a determination. In practical terms, these decisions mean that, in certain AECA prosecutions, prosecutors are well-advised to call not only a licensing official from DDTC, but also an expert from the Defense Trade Security Administration (DTSA), a component of the Department of Defense that assists DDTC in making determinations that commodities are defense articles subject to the ITAR.

United States v. Pulungan, 569 F.3d 326 (7th Cir. 2009), involved a defendant who was convicted of attempting to export riflescopes to Indonesia without having first obtained a license from DDTC. At trial, the Government called a witness from DDTC, who testified that the type of riflescope in question was "manufactured to military specifications" and hence subject to the ITAR. *Id.* at 327. The witness did not explain what those specifications were or how the riflescopes satisfied them. The trial court agreed with the Government that AECA precluded any inquiry into whether DDTC had properly classified the commodity and instructed the jury that, as a matter of law, the riflescopes were ITAR items.

The Seventh Circuit reversed. *Id.* at 331. It found serious constitutional issues are created when the Government seeks to establish a critical fact by fiat, without supporting proof and without any evaluation from the judiciary or jury as to the sufficiency of such proof. *Id.* at 328. In addition, the court referenced the Supreme Court's holding in *United States v. Gaudin*, 515 U.S. 506 (1995), that the Fifth Amendment's Due Process Clause and the Sixth Amendment required the jury to decide each element of a crime beyond a reasonable doubt. *Pulungan*, 569 F.3d at 328.

It is possible to distinguish *Pulungan* on the ground that the court also ruled that the Government failed to prove that the defendant had acted willfully. It found that, although Pulungan believed his actions in trying to export the riflescopes to Indonesia were illegal, he based that conclusion on the mistaken premise that the United States had an ongoing arms embargo against Indonesia. In fact, the embargo had ended two years earlier. Accordingly, because Pulungan did not consider himself to be violating the AECA and the ITAR, the court found that he lacked the necessary mens rea. *Id.* at 329–31. Thus, it is possible to argue that *Pulungan*'s conclusions concerning the need to prove the justifications for classifying an item as a defense article under the ITAR are merely dicta. *But see Al-Bihani v. Obama*, 619 F.3d 1, 2 (D.C. Cir. 2010) (Brown, J., concurring) ("It is a longstanding principle that alternative holdings each possess precedential effect.").

United States v. Wu, 711 F.3d 1 (1st Cir. 2013), is less easy to distinguish. Wu and his ex-wife, Yufeng Wei, were charged in a multi-count indictment with, among other offenses, violating the AECA by twice exporting to China without a license ITAR-controlled "phase shifters," electronic devices that can alter frequency waves and are designed to military specifications. *Id.* at 11–12. At trial, the Government did call an expert "regarding the design and the use of phase shifters." *Id.* at 14. However, at the conclusion of the case, the district court "told the jury that it should only decide 'whether the government has proved beyond a reasonable doubt that the Secretary of State determined that the charged parts were defense articles on the Munitions List at the time of export.' " *Id.* at 18. The jury thus was not to decide independently whether the phase shifters in fact qualified as defense articles subject to the ITAR.

The First Circuit reversed, finding the trial court's jury instruction violated the defendants' Sixth Amendment rights: "[T]he government may not decide for itself that some prior act by a criminal defendant violated the law, and thereby remove that determination from the province of the jury." *Id.* at 8, 17.

Pulungan and *Wu* demonstrate the perils in failing to put on proof, likely from an expert, as to why DDTC has determined that a commodity is subject to the ITAR. The two cases also highlight the dangers in seeking to give the jury an instruction that fails to ask it to decide whether the commodity is a defense article. *Wu* does suggest a possible exception to its holding. What particularly troubled the court was that DDTC's decision that the phase shifters were defense articles was made after the exports occurred. *See id.* at 17 ("[T]here would be serious constitutional problems if we read [AECA] to render Directorate determinations issued *after* exports have already occurred as being retroactively dispositive as to the coverage of the Munitions List.") (emphasis in the original). The *Wu* panel contrasted the situation it faced with that before the Ninth Circuit in *United States v. Spawr Optical Research, Inc.*, 864 F.2d 1467 (9th Cir. 1988), where the Department of Commerce had already classified the items being exported as subject to its licensing requirements before the exports happened. *Wu*, 711 F.3d at 19. Thus, the First

Circuit might have decided the issue differently in *Wu* if the commodity at issue was one that DDTC had previously reviewed and determined to be subject to the ITAR. The riflescopes in *Pulungan* also might have fallen within the exception *Wu* suggests.

This issue may ultimately become less important as the Administration's export reform program comes into being. As noted above, the ITAR's Munitions List currently consists of very broad categories of commodities that encompass a vast array of defense articles and their components. The ITAR is being revised to consist of "a 'positive list' of specific controlled items in place of its current catalogue of generic descriptions." *Id.* at 20 n.11. In addition, many less sensitive items are being transferred to the Commerce Control List (CCL) and the jurisdiction of the Department of Commerce. *See generally* PRESIDENT'S EXPORT CONTROL REFORM INITIATIVE, *available at* http://export.gov/ecr/. As described below, proving that an item is on the CCL is less complicated than demonstrating for many commodities that they are defense articles subject to the ITAR.

Nevertheless, in light of the Supreme Court's trend in recent years to accord ever more protections to a defendant's Sixth Amendment rights, *see, e.g.*, *Apprendi v. New Jersey*, 530 U.S. 466, 497 (2000); *United States v. Gaudin*, 515 U.S. 506, 517, 522 (1995), the most prudent course for an Assistant U.S. Attorney to take is to offer proof as to why a commodity satisfies the requirements for inclusion on the ITAR and to avoid jury instructions that appear to remove the issue of an item's status as a defense article from the jury's consideration. Of course, before offering a jury instruction pertaining to any of the export statutes, prosecutors should consult with the Counterespionage Section.

It is also worth noting that presenting evidence in support of DDTC's conclusion that an item is a defense article may also strengthen your case and increase its jury appeal. Under the current regime, many defense articles are discrete components, and it is not always obvious how they are crucial to the operation of a weapons system. In a case I handled, *United States v. Sudarshan*, Criminal No. 07-051 (RMU) (D.D.C. 2006), the defendant was charged with illegally exporting multiple items in violation of the AECA and the ITAR. Among the items was an i960 Intel Microprocessor (i960). Its intended use was in the navigation and weapons guidance system of a combat aircraft that the Indian government was developing. The defense argued that the i960 was similar to the microprocessor that powers an Xbox. However, the DTSA expert would have testified—had the defendants not pled—that the i960 had qualities that demonstrated it was specifically designed for military applications and, in particular, that it was built to withstand extreme g-forces and to function at altitudes of 50,000 feet or higher. Even the roughest teenager could not expose an Xbox to such conditions.

B. Cases charging violations of IEEPA and EAR

The Department of Commerce, through the EAR, regulates the export of dual-use commodities, that is, products that serve both military and civilian functions. Within the EAR, these items appear on the CCL. *See* 15 C.F.R. § 774.1 (2013). Unlike the current Munitions List, the CCL is a "positive" list. For each product that appears on the CCL, there is a corresponding set of specifications. Accordingly, to demonstrate that an item is on the CCL, it is necessary to do a comparison between the good's specifications and those in the CCL. A Department of Commerce licensing officer can provide such testimony. Most of the licensing officers have an engineering background and some technical expertise. It is probably wise to notice them as experts, although their testimony is not really going to involve much in the way of true opinions.

The fact that an item is on the CCL does not end the inquiry. For every controlled commodity, the CCL also identifies the type of control to which the product is subject. For example, some goods are controlled for national security reasons (designated as NS in the regulations), others are controlled for anti-terrorism reasons (designated as AT in the regulations), and still others are controlled for nuclear nonproliferation reasons (designated as NP in the regulations). These designations are not an exhaustive list of all of the types of controls. The next step in determining whether a controlled commodity requires a

license under the EAR before export is to compare the end destination for the product with the types of controls to which it is subject. This comparison is done by consulting the country chart, which identifies for each country which types of controls apply to exports to that nation. *See* 15 C.F.R. § 738, Supp. 1 (2013). If the chart indicates that certain controls apply to a particular country, a license is generally required for any good subject to those types of controls exported to that country. For example, according to the country chart, a license is required for any item that is subject to nuclear nonproliferation (NP) controls that is being exported to Pakistan. That requirement does not apply if the same product is being exported to, say, South Africa.

The Department of Commerce licensing officer will be able to explain the different controls and the working of the country chart. Based on a review of the Department's database of licenses, he or she will also be able to testify to the failure of your defendant to obtain the necessary license.

The Department of Commerce oversees a few areas involving blanket sanctions. In these situations, an item's presence on the CCL is often irrelevant to whether it can be exported. For example, the Department of Commerce is primarily responsible for the Government's sanctions against Syria, which consist of an almost outright ban on all exports to Syria without a license, with the exception of food and medicine. *See* 15 C.F.R. § 746.9 (2013). The EAR also include the Entity List (15 C.F.R. § 744, Supp. 4), which precludes the unlicensed export of certain commodities to various foreign parties engaged in activities contrary to U.S. national security or foreign policy interests, especially those activities involved in the development of weapons of mass destruction and their delivery systems. In addition, the Department can deny export privileges to particular individuals or organizations. Such individuals or entities appear on the Department of Commerce's Denied Persons List. *See* DENIED PERSONS LIST, *available at* http://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/denied-persons-list. In cases involving each of these types of controls, the licensing officer will be able to say, based on a review of the Department's records, whether the Department of Commerce ever issued a defendant the necessary license or, in the case of Denied Persons, gave approval to export.

C. Cases involving violations of IEEPA and OFAC's various sanctions regimes

The Department of the Treasury, through OFAC and its authorities under IEEPA, administers a variety of sanctions programs against countries, regimes, and individuals whose actions are deemed to be contrary to the national security, foreign policy, and economy of the United States. Most common of these are the Iranian Transactions and Sanctions Regulations (ITSR) (31 C.F.R. §§ 560.101–.803), the Cuban Assets and Control Regulations (31 C.F.R. §§ 515.101–.901), and the North Korea Sanctions Regulations (31 C.F.R. §§ 510.101–.901). OFAC also administers the Specially Designated Nationals List.

Because these are very broad-based sanctions programs, the issue at trial, in terms of licensing, will be whether the charged transaction falls within the relevant program's sanctions and, if so, whether the defendants ever obtained a license for that transaction. For example, the ITSR bans "the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, technology, or services to Iran or the Government of Iran." 31 C.F.R. § 560.204 (2013). Therefore, if your defendant, the vice-president of global sales for an American company, was involved in sending products to Iran via a third country, the only question for the licensing officer will be whether the vice-president had ever obtained a license for the transaction(s). The licensing officer will not have to demonstrate that the underlying commodities possessed qualities that rendered them subject to export controls. That Iran is the ultimate destination of the shipment is (assuming willfulness) what makes the export unlawful. Through a check of OFAC's database, the licensing officer will be able to say whether the defendant ever acquired the necessary license.

III. Suggested topics to cover with a licensing officer

Because in most cases a licensing officer is being offered to give testimony on a narrow subject—whether the defendants have a license for the charged transaction(s)—the amount of additional testimony that you will be able to elicit from the witness will depend on your judge. You may run into difficulties if you try to have the witness explain or interpret the regulations, because the defense can argue—and the court could accept—that such matters are purely legal and solely for the judge to instruct the jury.

Nevertheless, there are some topics that most judges should permit you to explore beyond the witness' experience and qualifications and his or her search for licenses. One important way the licensing officer can help the prosecution is to dispel the notion that the defense always pushes, which is that the regulations are unduly complicated and the actions of the licensing agencies are opaque. At the outset of the direct examination, the licensing officer can give a good description of the organization of the licensing agency and its various responsibilities. The witness should also be able to define certain key terms (for example, an explanation of the Munitions List or CCL, or a general description of the sanctions regime at issue in the case).

With respect to the Munitions List and the CCL, the licensing officer should be able to describe the process by which an item gets placed on either list. The witness can explain how various parts of the Government—the Departments of State, Defense, and the Treasury, as well as the Intelligence Community—weigh in on the decision as to how to classify a product. The witness can also explain how input will be sought from industry and from a product's manufacturer. In addition, the court should permit the licensing officer to talk about the process for challenging a determination that an item is controlled.

In order to further demonstrate that the three licensing agencies are transparent about their activities and requirements, the licensing officer can talk about the "commodity jurisdiction" or "commodity classification" process at DDTC and the Department of Commerce, respectively. These programs allow manufacturers and sellers of products to ask DDTC or the Department of Commerce to determine whether a product belongs on the Munitions List or the CCL, or whether it is not subject to such controls. The licensing officer will make clear that, as part of this process, each agency will solicit the views of the other so as to prevent conflicting rulings. The witness can also demonstrate how easy it is to find information on getting determinations from DDTC and the Department of Commerce on their Web sites, as well as information on export restrictions in general. Similarly, the OFAC Web site provides helpful information on how to comply with the sanctions regimes. Each of the licensing agencies routinely has outreach and training sessions for industry and individuals across the country throughout the year, as well. Indeed, it is noteworthy how often agents find evidence of a defendant attending such a session in the course of a search, or how often visits to one of the agency's Web sites appear in a defendant's browsing history on his computer.

It is also a good idea to have the licensing officer show the jury both a model license application and a model license. The application will demonstrate the Government's interest in the end-use and end-user of the product, and the witness should be able to explain how that information is useful to the Government in deciding whether to authorize the export. The license itself will show exactly what an exporter can be authorized to do. The model exhibits should highlight how, in many cases, the front companies and transshipment ports procurement agents often serve only one purpose: the willful evasion of important U.S. export controls.

The next important subject area to cover is the case-specific determination that a license was necessary for the export(s) being charged. Even in the case of defense articles subject to the ITAR, where DTSA will have done the technical analysis of the product, DDTC still makes the ultimate decision—that an item is on the Munitions List—based on that analysis. Thus, the DDTC licensing officer will have to testify that a license was necessary for the export(s). The Department of Commerce and the OFAC

licensing officers will give similar testimony for the products and transactions under their agencies' purview.

Last, but not least, one must not forget to ask the licensing officer the question for which he or she is a witness in the first place: Did the defendants have a license for the export(s) underlying the charge(s) in the indictment? The answer, of course, will be in the negative.

In the end, the licensing officer will have assisted you in establishing one of the elements of the offense. In the process, however, you also will have further demonstrated to the jury why a product cannot be exported without a license, why such a control is important to the national security and foreign policy of the United States, and frequently why your defendants have acted willfully.

IV. Outline of questions for Department of State/Directorate of Defense Trade Controls

At base, such a witness is called to establish:

(1) The licensing requirement of the AECA/ITAR generally and specifically for the particular defense article or defense service,

(2) The DOS/DDTC registration and licensing process,

(3) The fairness and transparency of that process (that is, regarding notice and determinations),

(4) The certification or determination by the DOS/DDTC that the relevant article/service at issue in the trial was on the Munitions List, and

(5) The defendant's and his conspirators' lack of an export license or authorization from the DOS/DDTC.

A. Background

- Education
- Training: on the job, classroom, etc.
- Experience: government, private industry, military
- Publications

B. DOS/DDTC and the work of a licensing official

- What is the Directorate of Defense Trade Controls?
- What is the nature of the work? Various sections and responsibilities?
- A few details or examples of the work of the DDTC

C. AECA, ITAR, and the Munitions List

- In very general terms, what are the following: the AECA, the ITAR, the registration requirement for manufacturers and exports of munitions, the Defense Articles (technical data) or Defense Services, and the licensing requirement?
- What is the Munitions List?
- Who creates it and determines its content?
- What is included? Description of a few categories, chart, and relevant category for this particular prosecution.

- How is the USML organized?
- Where is it? How does one access it? DDTC Web site, etc.
- Is there input from industry or manufacturers of munitions and private citizens with regard to the Munitions List and its composition?
- Is there a process for challenges to items being included within the Munitions List?
- What is that process? Without paying any fees or costs, is one able to submit such challenges or proposals for changes?
- Are changes or modifications made to the Munitions List as a result of input from companies and individual private citizens?
- Ultimately, who has Congress authorized to control what items are on the Munitions List? The President as Commander in Chief of the military and nation.

D. The license process

- What is it?
- What is licensed?
- An example or model license: Blank Form
- In general, what type of information is sought?
- Why is that information sought? How is that information useful to DOS, DOD, and others in the licensing determination (and otherwise)?
- Who is involved in that process?
- Which agencies?
- What is the role of DOD/DTSA?
- What is DTSA?
- How is that input from various agencies included?

E. Public notice and fairness

- Public inquiry
- Is there a means by which private citizens or companies which export or manufacture munitions may obtain an opinion or review of whether they need an export license from DOS for a particular item or to provide a particular service to a foreign country?
- What is the Commodity Jurisdiction process?
- How does that process work generally?
- If a citizen disputes the initial determination, is there a means or process by which he or she may protest that determination and obtain further review?
- Is that system of informal review and determinations about licensing requirements written out and publicly available? Where? The ITAR.
- Are these rules and procedures available publicly? Where? The ITAR and the Web site?
- Examples from the Web site

- What is maintained on the Web site? What types of information are available?
- Examples
- What other types of public notice are provided?
- Conferences? Press notices? To newspapers and in trade journals?

F. License determination

- Was DOS/DDTC asked to determine whether Widget X is a defense article and on the USML?
- When and how asked?
- What was done with that inquiry?
- Describe review process within DOS/DDTC and DOD.
- What determination was made?
- Was that recorded?
- The Certification
- What does it state and what was determined?
- Is Widget X on the Munitions List?
- Is a license or authorization from the DOS/DDTC required to export Widget X from the United States to a citizen of Country A or to Country A?
- If a proscribed country under 22 C.F.R. § 126.1 (2013): Has it been prohibited to export any munitions to certain countries? A few examples. Is Country A among those prohibited countries? Is that prohibition publicized? How? The ITAR, Web site, training, conferences, etc. Since when has that prohibition been in place?

G. Lack of license

- Was DOS/DDTC asked to determine whether the defendant Mr. Jones was registered with the DOS/DDTC as a manufacturer/exporter?
- What was done in response to that inquiry? General description of data base and record keeping of DOS/DDTC of registrants?
- What was found?
- Was DOS/DDTC asked to determine whether the defendant Mr. Jones ever obtained a license to export a defense article/service to a foreign national or foreign citizen?
- What was done in response to that inquiry? General description of data base and record keeping of DOS/DDTC of export licenses?
- What was found?
- Did defendant Mr. Jones ever apply for and obtain a license or authorization to export Widget X to Country A or to a citizen of Country A?
- Did defendant Mr. Jones ever have an export license or authorization from the DOS/DDTC for the export of Widget X or any other munitions or defense article?
- The Certifications

- If there is a prior registration or licensing history for that person or company, then ask questions to review that history as relevant to determine knowledge of the licensing or registration process, the DOS/DDTC licensing requirements, the DOS/DDTC resources to answer questions, etc.❖

ABOUT THE AUTHOR

❑ **Jay Bratt** is the Deputy Chief of the National Security Section in the U.S. Attorney's Office for the District of Columbia. At the U.S. Attorney's Office, he has prosecuted a wide variety of Espionage Act, export enforcement, and counterterrorism matters. Mr. Bratt has also served as the National Security Counselor for ICE, Deputy Director of the Guantanamo Review Task Force, and Chief of the Litigation Section in the Office of Intelligence at the Department of Justice, where he oversaw requests for the use of FISA and FISA-derived information in connection with judicial and other proceedings. ✠