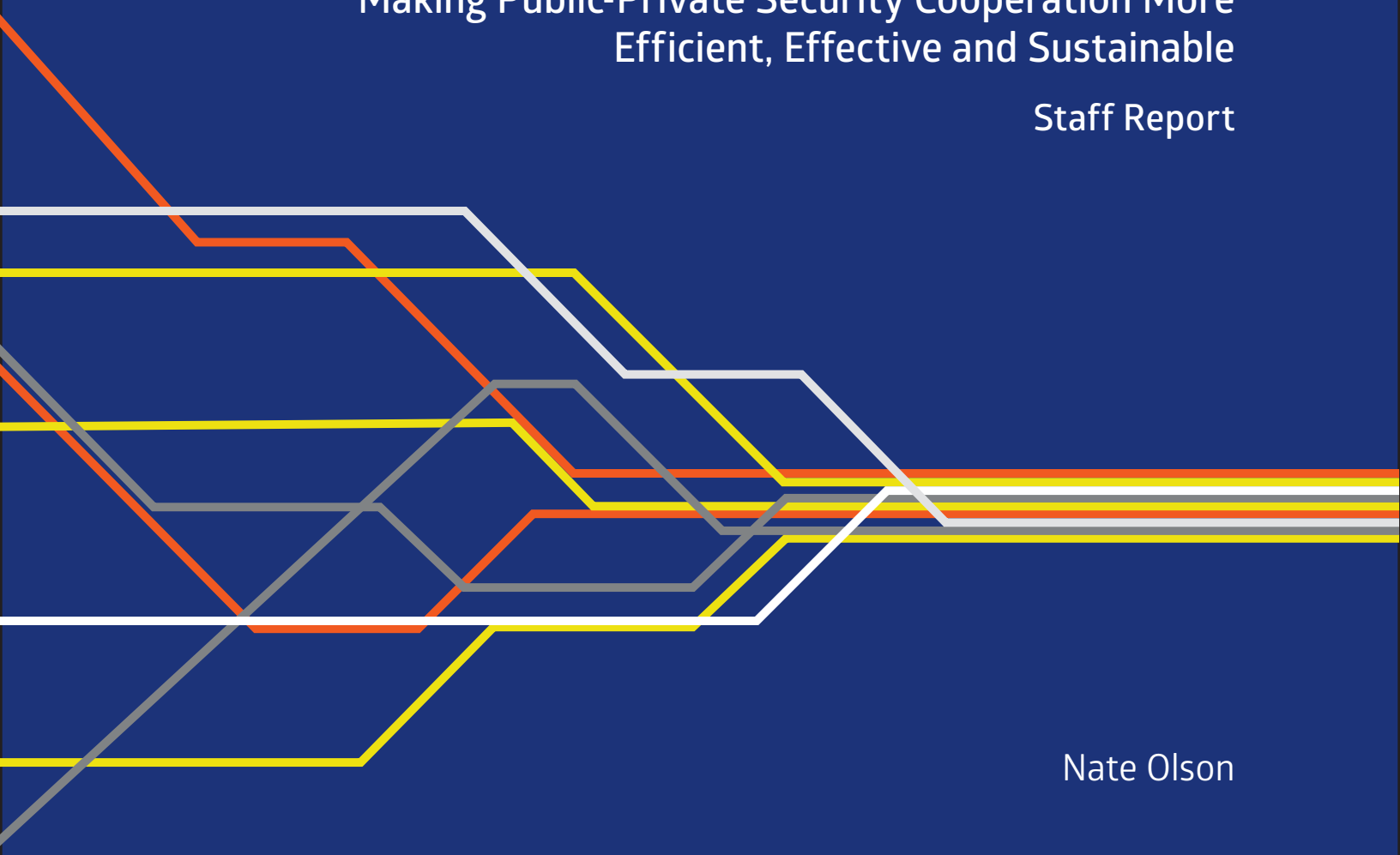
STIMSON

Partners in Prevention

Making Public-Private Security Cooperation More Efficient, Effective and Sustainable

Staff Report



Nate Olson

December 2014

Preface

In May 2014, Stimson's Partners in Prevention Task Force endorsed seven proposals to close security gaps in global trade by better leveraging market incentives. Directed mainly at US policy and industry stakeholders, those recommendations were the result of an 18-month collaboration with high-tech manufacturers and service providers, transport and logistics firms, and insurance providers. In addition to ongoing individual interviews with private sector representatives, Stimson convened several closed-door industry roundtables on topics of special interest. Stimson also periodically briefed US government officials to ensure the relevance of the final Task Force proposals and to strengthen the partnerships crucial to the implementation phase now underway.

Supporting all of these efforts was a first-rate project team at Stimson. I am pleased now to present this report, which is based on the various research and analytical products prepared by the project team for the Task Force, as well as numerous interviews with industry. As such, it largely reflects events prior to May 2014, though it has been updated in select cases to account for more recent developments. It also parallels the Task Force proposals in its focus on exports as an area critical to global trade and security issues.

While the Task Force recommendations were highly targeted and prescriptive, this report covers a much wider substantive range and elaborates key background issues. In so doing, it lays bare the urgent need to modernize public-private partnerships for a 21st-century economic and security environment. In collaboration with stakeholders from government, industry and civil society, we look forward to continuing this important work.

Brian Finlay
Managing Director, Stimson

The 21st-Century Threat Environment

GLOBALIZATION, ILLICIT TRAFFICKING AND WMD

The catastrophic events of September 11, 2001, led to a reordering of American national security priorities. Terrorism involving the use of nuclear, biological or chemical weapons of mass destruction (WMD) emerged as a preeminent national security concern and as a national cause célèbre demanding robust budget authorities and programmatic efforts. But in the years since, it has been clear that the forces of globalization pose a fundamental challenge to even the most committed governments looking to acquire WMD-related materials, technologies and know-how by would-be proliferators. Despite all their benefits, cross-border financial flows, telecommunications, and private sector business models have empowered terrorists and criminals on a new scale.

THE RISE OF GLOBAL VALUE CHAINS[1]

After building over several decades, an array of powerful economic and political forces have now converged to dramatically expand access to dual-use knowledge and equipment.

FDI growth. While foreign direct investment (FDI) had long been viewed with suspicion by governments around the world, by the 1980s many concluded that it yielded not only short-term financial gains but also long-term economic benefits. The global development community joined economists and state development agencies in promoting to the governments of less-developed countries models of export-oriented growth jumpstarted by outside investment. FDI rose from $14 billion in 1970 to $1.46 trillion by 2013.[2] More countries have enhanced domestic capabilities for the manufacture of weapons of mass destruction and their means of delivery — as well as for the export of such capabilities.[3]

Advent of global corporate structures. As private companies in the developed world gained access to new technologies, they sought to maximize profit and efficiency through outsourcing, off-shoring, and other changes to business models that drove intellectual and manufacturing capacity well beyond Western shores. The corresponding transfer of technologies and information led to new local enterprises, including subsidiary operations, competing for global market share. Soon, states that were thought to have lacked the indigenous expertise to perform complex R&D and manufacturing operations began to develop competitive industrial sectors.[4]

Spread of innovative manufacturing capacities. The Global Innovation Index shows that knowledge and wealth creation continue to be led by the United States, Germany, the United Kingdom, and Japan, but other indicators suggest an emerging innovation capacity among newly industrialized and even developing world economies. The biological sciences are particularly telling. Cuba, for example, was one of the first countries to have developed a vaccine against group B meningococcus. Egypt has developed several innovative diagnostic and therapeutic products for hepatitis C. India developed and now produces a recombinant hepatitis B vaccine and is one of several developing countries, including Brazil, which has launched a major nanotechnology initiative.[5]

Accelerated movement of goods. Reduced tariff barriers and modern communication and transportation technologies now allow companies to ship products and information around the world at great speed.[6] The United Arab Emirates (UAE) alone invested billions of dollars in the 1990s to

become a global trading hub. By 2012, more than $22 billion in US goods flowed through the UAE annually.[7] The sheer volume of trade transiting these ports runs up against practical limitations in legal and regulatory tools, as well as the larger strategy of technology denial.

Increased cross-border trade in services. Supporting and augmenting this increased trade in goods has been an increase in international services — from transport, telecommunications and energy to finance, insurance and tourism. Services have increased in importance to the world economy both in developed and developing countries.[8] US exports in services increased in 2012 to many key trading partners — including an estimated $61.2 billion in private commercial services to Canada alone, an increase of more than 145 percent from 2002.[9] Additionally, US exports of services to the European Union (EU) in 2012 were estimated around $194 billion — a 108 percent increase since 2000.[10] This represents a relatively under-researched threat area as well as an under-utilized area for targeting the prevention of illicit transfers in both services and related goods.

The New Era of Illicit Trade and Proliferation

Illicit trafficking thrives on this globalized economy. It can include almost any product, from dual-use technology and materials to conflict diamonds, timber or narcotics. Where there is demand, there will be someone willing to supply.

But not all illicit commodities are created equal. While the smuggling of some products is merely an irritant to local law enforcement, the shipment of other commodities can have dramatic national security and geopolitical repercussions. For not only does illicit trafficking provide terrorists with funding to pursue their attacks, it can also supply them and other non-state actors and rogue nations with sensitive WMD and military technology that can be used against US interests and allies.

In our modern economy, the threat of illicit trafficking is inextricably connected to the threat of proliferation. It is true that WMD items are a separate and distinct trade from pharmaceuticals, counterfeit t-shirts and other illicitly traded goods. It also is true that most coca farmers and human traffickers will never become proliferators. But it also is true that each of these contraband flows transits the same global supply chain — in the bellies of the same aircrafts, in the holds of the same ships, at the same ports of embarkation and arrival, and facilitated by the same freight forwarders and underwritten by the same insurers.

This convergence represents a unique opportunity to better focus enforcement resources to choke off all manner of contraband as it intersects licit global value chains.

Increased access to proliferation-sensitive items remains a grave concern for the United States. A Department of Justice compilation of select export violations highlights many examples, such as the export of gas centrifuges and vacuum pumps to China and Iran. These cases often entail false declarations of end-users and other commodity or shipping manifest data.[11] The export of these items is especially disconcerting as more countries, including Iran and North Korea, continue to enhance their nuclear weapons capability.

For governments, illicit trafficking is not only a security threat. It is an economic challenge. To understand the economic impact of illicit trade, it is helpful to break down the economic costs by type of good. In the illicit drug market, Justin Picard, co-founder of Black Market Watch, estimates that for every dollar spent (direct impact) in the procurement of illicit drugs, $1.54 is incurred in indirect costs by society, including prevention, healthcare costs, law enforcement and the negative impact on societal productivity.[12] Thus the US illegal drug trade had an imputed economic impact of $516 billion

in 2002.[13] Because there is scant research on the economic impact of illicit trade in other commodities, Picard expands this methodology to other trafficking flows, applying the same ratio of 1.5.[14] Picard thus estimates that in 2005, human trafficking had a monetary impact of $128 billion in the US.[15]

At a time when global economic and political forces require tighter collaboration between governments and industry, relationships between the public and private sectors in most countries, including the United States, are often tainted with mutual suspicion and animosity. Making these relationships more functional is paramount in preventing WMD proliferation in the 21st century.

CONVERGING THREATS IN ILLICIT TRADE

Growing evidence suggests that human traffickers in Eastern Europe, drug traffickers in South America, illicit arms traders in Africa, and terrorist cells in East Asia often collaborate for mutual benefit while evading state-based regulatory authorities. Their activities are facilitated by global supply chains whose complexity makes them impossible for any government, or even consortium of like-minded governments, to fully understand and address. In modern national security parlance, this is referred to as "threat convergence."

What [drug-trafficking organizations] are really selling is logistics, much like Wal-Mart and Amazon.com…and illegal drugs are but one of the products they offer.

Evelyn Krache Morris
"Think Again: Mexican Drug Cartels"
ForeignPolicy.com
December 3, 2013

COMMON PATHWAYS

Trafficking groups increasingly draw on the same playbook.[16] As noted above, we have yet to see ample corroboration of a common clientele between WMD traffickers and purveyors of other transnational flows of contraband. What is clear, however, is that nuclear, biological and chemical weapons components traverse many of the same transit nodes and conveyances as other forms of illicit goods. Thus while the extreme ends of the global supply chain (manufacturers and end users) look very different in the WMD context than in that of other contraband, the wide middle of that supply chain is in many cases shared.

Increasing participation of criminal actors in proliferation networks demonstrates that the supply chain connecting dual-use producers to dual-use recipients overlaps with those of other illicit items. While drug smugglers, for instance, are unlikely to become nuclear terrorists themselves, the illicit transportation networks they build are also leveraged to support state-based proliferation programs and generate funds to support terrorist activities and rogue regimes. [17]

The tri-border area of Argentina, Brazil and Paraguay is infamous for arms and drug smuggling, money laundering, human trafficking and other illicit activities. Some of the resulting funds support terrorist groups, such as the Iranian-backed Hezbollah.[18] There also is concern that Brazil and Argentina have sophisticated nuclear technology that could be of interest to terrorist groups or their state supporters.[19]

Hezbollah has also forged relationships with Latin American drug cartels, including the Zetas, to traffic arms, increase revenue and build a stronger foothold in the Western Hemisphere. Lebanese

diaspora communities in Latin America linked to Hezbollah move cocaine from Colombia to Mexican cartels.[20] Some analysts hold these Hezbollah activities to be a major national security concern, contending that the proceeds they generate provide "the oxygen for any action, legal or illegal — and more importantly for…lethal operations."[21]

Illicit trafficking can also be a tool employed by nations whose economic and political options are constrained by international sanctions or other headwinds. Office-39 (or Bureau-39) is a state-run international illicit supplier for the Democratic People's Republic of Korea (DPRK) providing drugs, weapons and counterfeit materials to the global illicit market.[22] Earnings from Office-39 are used to prop up the regime, procure military technology, and fund North Korea's WMD programs.[23] The paths of illicit trade further converged when Office-39 supported the rebels in Myanmar in the early 2000s, supplying weapons and acting as middleman in the Southeast Asian heroin trade.[24]

The clandestine world of illicit trafficking is not the only trade-related security challenge brought into sharp relief in recent years. Another category of threats pairs illicit trade with deliberate compromises to the physical and informational infrastructure of legitimate commerce. Cybersecurity, in particular, arguably represents a new dimension in the threat environment. Industry is seeing significant losses from criminals fraudulently posing as legitimate truckers on web-based "load boards" that match cargo with spare trucking capacity. Drug traffickers hacked into the port of Antwerp's IT system to move its product to a growing list of onward destinations for two years before being caught. And importer identity thefts have been a problem for US Customs and Border Protection (CBP).[25] There is significant potential that such breaches will cause major disruptions in the coming years.[26]

Finally, there sometimes are very overt acts of aggression and violence against trade stakeholders. Maritime piracy is but one example. In addition to the violence it can visit upon legitimate trade stakeholders, piracy of course also funds terrorists, renegade state actors and gangs.[27]

PATTERNS OF PROLIFERATION

Illicit trafficking also fosters the diffusion of dual-use technology among nations and groups of international concern. Sanctioned countries rely on suppliers around the world for materials for their nuclear weapon and other WMD programs. These countries now have more access to critical know-how, materials and capacities to develop, build and ultimately use weapons of mass destruction today than ever before. More important, the number of private companies servicing this global market has also expanded. The techniques involved in WMD development — harnessing of the atom, synthesizing chemical production, and using biological organisms or substances — have a legitimate and, indeed, necessary use in the civilian economy.

The same is true for the development of many WMD delivery methods, from aerial vehicles to atomizers. Thus the environment in which proliferation risks occur is shaped largely by the private sector. Privately owned companies not only produce and operate nuclear, chemical, and biological industrial equipment, but also carry out, by far, the greatest share of the basic R&D for relevant technologies, goods and methods of application. In addition, university research is often commercially funded, and governments have expanded public-private partnerships even in some of the most sensitive areas of technology in order to take advantage of cost reductions and innovation.[28]

To build its chemical weapons program, Syria utilized front companies and illicit suppliers from Europe, the United States, and the Middle East. Until 2003, Syria was supplied nerve agent VX by former Soviet General Anatoliy Kuntsevich, and experts point towards illegal front companies in Iraq and Iran involved in supplying the needed dual-use chemicals necessary for sarin gas.[29] Syria was also

able to obtain precursor chemicals for chemical weapons "legally" from multiple, licensed suppliers for many years.[30]

Both the DPRK and Iran's nuclear and ballistic missile programs have been long sanctioned by the UN and as a result have developed supportive illicit networks to continue their nuclear programs. The DPRK developed a significant non-nuclear covert smuggling capability that has also aided in the transfer of sensitive items into and out of the country.[31] The Korea Mining and Development Trading Corporation (known as KOMID), which exports minerals, is also responsible for the export of certain weapons, particularly technologies and materials linked to ballistic proliferation. Notably, it has been confirmed as the entity through which ballistic technologies were transferred to Iran.[32] Similarly, despite significant economic sanctions, the Government of Iran itself has managed to rely upon illicit networks to obtain critical technologies for their uranium enrichment program.[33] In addition, countries including China are using illicit networks to procure weapon technology that the US has refused to export.

The unregistered and unfettered proliferation of military and dual-use items is a national security concern for the United States. The range of items contributing to WMD development is large, as is the number of countries seeking those items.[34] Although these cases are rightly viewed as significant challenges for global nonproliferation efforts, they might also be considered opportunities to leverage both lessons learned and tangible programmatic efforts in adjacent counter-trafficking industries to mutually promote global WMD prevention efforts.

Another Example: The Radiopharmaceuticals Sector

The risks attendant to radiopharmaceutical production are technically complex and atypical in some ways, encompassing issues from global security to health care.[35] Most radiopharmaceuticals are produced in research reactors fueled by enriched uranium, which, for many years, has been nuclear weapons-grade, highly enriched uranium (HEU). The civilian sector uses these radioisotopes in a variety of applications. For example, radioisotopes derived from HEU-fueled reactors are used by health care professionals for diagnostic medical procedures, such as scans of the heart, bone, brain, thyroid, lungs, liver, spleen, kidney, tumors and more.[36] Moreover, the "targets" bombarded in these reactors to produce the isotopes are also composed of weapons- or near-weapons-grade enriched uranium. Much of this production has been converted to employ uranium of less than 20 percent enrichment, commonly called lower-enriched uranium (LEU).

Radiopharmaceuticals:
Three Types of Threats

WMD Proliferation: A country or non-state actor could use enriched uranium to produce isotopes for weapons of mass destruction.

Transport: Nuclear materials may be diverted accidentally or through theft, putting these materials into the hands of rogue states or non-state actors

Radiopharma Supply: Breakdown of aged reactors could cause severe shortages.

Even at this lower level of enrichment, however, there are significant proliferation risks. There is potential for these radioisotopes to be diverted by individuals for acts of nuclear/radiological terrorism. Moreover, the conversion of reactor fuels and targets from HEU to LEU, which is not yet complete and entails significant technical problems and economic costs, does not preclude reasonably rapid re-enrichment of the fuel to nuclear weapons grade, which has been a key issue in the nuclear negotiations with Iran.

Non-nuclear weapons states like Iran have claimed to need enriched uranium to produce isotopes for local and regional medical markets. The international community has struggled to address this key nonproliferation issue over recent decades. Options such as substituting LEU as fuel have been widely discussed, but serious technical and economic challenges remain.

Moreover, since the few reactors making these isotopes are old and in frequent need of repair, the supply chain of these isotopes is vulnerable to disruptions that result in severe shortages, skyrocketing costs, and delayed medical diagnoses and treatments. Basic scientific research suggests that it is possible to produce a new generation of isotopes without the use of reactors at all. Such non-fission isotopes may also have superior medical properties, resulting in substantial cost savings and improved health care.

However, the private companies seeking to develop and market these new drugs are stymied by costly and cumbersome regulations that provide strong disincentives for innovation. Yet there is potential for government and industry to accelerate the development of non-fission medical radioisotopes by invoking overriding nonproliferation imperatives, streamlining regulation and encouraging innovation in the private sector.

Actors in the Illicit Supply Chain and Their Methods

The array of private entities that could aid — either deliberately or unwittingly — the activities of a terrorist or committed state proliferator goes far beyond those firms that operate fuel enrichment facilities, experiment with select biological agents, or produce toxic chemicals. A broad swath of dual-use technology innovators and manufacturers are also involved in information security, telecommunications, sensors, lasers, and many other sectors that could have direct applications in proliferation efforts. Foreign trading companies, brokers, middlemen, shipping companies and freight forwarders are critical actors in moving materials and fabricated products. And underpinning all these transactions are financiers and insurers.

In the Shadows

Sometimes referred to as "shadow facilitators," these actors contribute, knowingly or unknowingly, to the trafficking of illicit and dangerous products across the globe. There are various levels of these facilitators, and their geographic dispersion ensures that if one part of the network is shut down, the other parts continue to function — in essence, creating a "network of networks."[37]

According to one analyst, these actors can be best categorized into three levels: fixers, super fixers, and shadow fixers.[38] Fixers are predominantly local financiers and suppliers, who provide the networks with in-demand goods. Super fixers aid the fixers by transporting the goods abroad. This group includes third party logistics service providers and carriers and includes the complicit and the unknowing. The shadow fixers offer further assistance — providing false documentation or undertaking cyber fraud to ensure the shipment of the goods. Super fixers make up the backbone of illicit trafficking. As mentioned above, super fixers may be unaware of the fact that they are contributing to the illicit trade, and are often co-opted by fixers or shadow fixers to import and export goods in and out of countries including the United States.

Suppliers of illicit goods often rely on fraudulent ordering schemes to embed their products within the legitimate trade flows, at once free-riding on the speed of modern supply chains and capitalizing on insufficient oversight and information sharing among authorities. Illicit traffickers exporting from the

US will often use multiple trade companies in various countries to disguise the ultimate end user. This is especially effective in the containerization process, and can feed on a lack of international information sharing as well as local corruption.

Suppliers will use false declarations both to hide end users and mask the container's contents. For example, from 2007-2008, a conglomerate of companies from Iran, Singapore and China used false declarations to disguise the final destination of telecommunications modules to be used in improvised explosive devices (IEDs) in Iran and Iraq. Believing that the final end user was in Singapore, the US exporter willingly sold the modules.[39] In another instance, from 2005-2007, two Dutch nationals provided false end-user certificates to US companies in order to acquire sensitive aircraft components destined for Iran. This case highlights the role of European middlemen in issuing false declarations and using EU end users as a cover before exporting onto the Middle East and Asia.[40]

Seventy-five percent of [the Commerce Department's top enforcement cases] involve elaborate procurement networks spread across multiple countries, including the United States.

US Department of Commerce
Bureau of Industry and Security
FY 2014 Budget Justification
March 2013

Front companies can effectively disguise the ultimate end user. In 2010, a Taiwanese national was arrested for illegally exporting dual-use missile components from the US to Iran, using a front company with ties to the Iranian Aerospace Industries Organization and the Iranian missile program.[41] The sheer volume of front companies in both Asia and the Middle East makes detection difficult for authorities and business compliance analysts. Industry suppliers face the daunting task of identifying front companies, which not only frequently change but also are often able to forge their credentials and status.

In order to overcome suspicion, as was evidenced in the use of Dutch nationals, illicit traffickers will often rely on Western facilitators, who are looked on with less suspicion. These individuals often fill the role of super and shadow fixers. In the EU, for example, once illicit products are within the borders, cargo is subject to less surveillance, especially for further export within the Union. Once within EU borders, illicit networks and corruption in Eastern and Central Europe ease the export of illicit goods into the Middle East and South Asia. Former Soviet Union countries are a black-box for illicit trade — where corruption and a lack of business transparency shroud the legitimate and illicit supply chains.

Industry Targets

The global financial system has rightly attracted a substantial degree of government attention for its role in facilitating proliferation networks. In 1989, recognizing the problem of illicit finance, the G7 established an international organization to coordinate policies regarding money laundering and terrorism finance, and protect the highly interconnected, international financial system. The resulting inter-governmental Financial Action Task Force focuses on establishing policies for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT).[42] Within the United States, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) works with financial institutions, mortgage brokers, jewelry dealers, insurers and with law enforcement to "safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities."[43]

Companies that unwittingly contribute to trafficking threats have been viewed by governments as part of the problem, rather than as potential partners. Likewise, companies in other sectors could either contribute to the proliferation supply chain or become a partner in its dismantlement. Some examples follow.

Technology Innovators

Identifying the breadth of technologies that could be diverted for weapons purposes is a massive task. Technology innovators include military and defense companies, satellite and telecommunications firms, as well as other companies that invest heavily in research and development such as DuPont, Pittsburgh Corning, General Motors, and Eli Lilly.[44] In today's dynamic world, even individual researchers can develop novel threats that governments want to control.[45]

Some companies, universities and research institutions establish close working relationships with government agencies and law enforcement in order to protect their intellectual capital and to protect themselves from export control violations. They also feel they are acting in their national interest, and are supported by US government efforts.[46] However, not all innovators feel the same way; thus the emphasis of developed world governments has been to erect barriers to the outflow and transfer of dangerous technologies, particularly since the 1990s. But sometimes regulations are lacking. Even more damaging, existing restrictions are unevenly applied globally — leading some to cite the negative economic effects on those countries with the best restrictions.

Manufacturing Sector

The producers of dual-use items have been particularly susceptible to unwitting exploitation by committed proliferators. The A.Q. Khan network most infamously exposed the degree to which legitimate companies could be so exploited, but it is far from the only instance. A host of criminal enterprises involving business activities are routinely exposed as they attempt to exploit the weaknesses in the global control regimes governing both WMD as well as conventional armaments.[47] Of course, Saddam Hussein took advantage of illicit networks and holes in regulatory regimes to circumvent the embargo and acquire goods from other countries for use in prohibited programs. In 1991, for example, while scouring an outpost in the desert of Iraq, UN weapons inspectors stumbled upon a small number of vacuum pumps made by the German manufacturing firm, Oerlikon Leybold Vacuum. At the time, none of the pumps appeared on any export control list.

On closer study, the inspectors realized that one of the vacuum pumps was attached to a cyclotron, which can be used to enrich uranium. Thus Oerlikon and their competitors had knowingly – though innocently — supplied the pumps to the government of Iraq and helped to advance its nuclear weapons program. As news of the case spread, the damage to the Oerlikon brand prompted the company to re-think the fulfillment of a growing number of suspicious requests for technology and develop an internal charter that would extend sales restrictions beyond that required by national laws. For dual-use manufacturers, this case illustrates the serious consequences that illicit networks may have on legitimate business operations. For government regulators, it points to the additional measures that industry could take — if given the incentive to do so — to support proliferation prevention.

The case of Oerlikon prompted an awakening, particularly among European companies and governments who have begun collaborative efforts to extend voluntary charters across a broad cross-section of dual-use industries.[48] Oerlikon has said it is trying to extend the so-called "Leybold Charter" across European dual-use industries. The Charter consists of a stringent set of voluntary

self-restraint mechanisms related to export matters and in support of nonproliferation objectives.49 This effort could serve as a model to North American and Southeast Asian countries where the threat of proliferation remains particularly acute. However, even with such a charter, companies will be faced with the dilemma of determining how much compliance with export controls and sanctions is enough: When are end-user checks sufficient?

Shipping Industry

Cargo carriers facilitate trade. A particularly egregious example of illicit transport is evidenced in Viktor Bout. In 1993, Bout, a highly trained and then-redundant officer of the Soviet military, founded a private shipping company called Transavia Export Cargo. Over the next two years, his fortunes grew to an estimated $50 million, aided in large measure by the delivery of weapons to the Northern Alliance in Afghanistan. Supported by multiple military aircraft obtained from Moscow, Bout's empire and profits grew as he moved his business operations from Belgium, where authorities had launched an investigation into his questionable activities, to the United Arab Emirates (UAE).

Using Sharjah International Airport as well as airfields in the neighboring emirates of Ajman and Ras Al Khaimah as transshipment points, Bout built a global network of front companies and clients. UN officials say that Bout smuggled untold numbers of small arms, narcotics and other contraband fueling African conflicts in Angola, Cameroon, Central African Republic, Democratic Republic of the Congo, Equatorial Guinea, Kenya, Liberia, Libya, Republic of the Congo, Rwanda, Sierra Leone, South Africa, Sudan, Swaziland and Uganda. Bout's operation exemplified the complexities of regulating the global shipping industry. Even the US government had become an unwitting client of Victor Bout when a freight forwarder under contract to the State Department subcontracted to his firm.[50]

Because of Bout's continued ties to the Russian military, Western intelligence agencies were particularly concerned with his potential to move contraband nuclear material into Afghanistan. While the CIA never received credible evidence of WMD material shipped on Bout's planes, allegations from a senior Afghan official did suggest that Ariana Airlines shipped cyanide, ricin, and other toxic substances for al Qaeda from Sharjah to Kandahar.[51] Although it would appear that the "merchant of death" was not a party to the WMD supply chain, his network illustrates that the global shipping industry extends well beyond the much publicized sea-based cargo container market around which extensive government outreach at targeted "megaports" is occurring. Bout is now serving a 25-year sentence in the United States.[52]

Without the willingness of this industry to not only know their customer but also know their cargo, preventing the diffusion of materials and weapons of mass destruction will become increasingly more challenging. It is incumbent on governments to appropriately encourage more rigorous industry practices through market-based incentives.

Other Trade Facilitators

Like financiers, other trade facilitators play an important role in managing trade and seeing the breadth of transactions taking place, both legal and potentially illegal. This includes brokers and distributors, the insurance industry, and third party logistic providers such as freight forwarders. Attention has only been marginally given to these industry stakeholders and their roles in proliferation.[53] Yet they play a central role in illicit trafficking.

One recent example involves the Standard Club, a mutual insurance company that provides its members third-party liability coverage for ship operations.[54] After it learned from intelligence

services that a Russian ship it insured was carrying weapons to Syria, the insurer withdrew coverage on that and seven other ships of the Russian fleet owner. This avoided the insurer being in violation of European Union sanctions and caused the ship to turn around.[55]

SELECT TRENDS

Illicit trade in proliferation-sensitive items remains a grave concern for the United States. A Department of Justice compilation of major export violations highlights many attempted exports of dual-use items and defense articles to destinations including China, Iran and Pakistan.[56] These violations typically involve false declarations of end users, end uses, or both. In recent years, however, many in government and the expert community have flagged a growing connection between such cases and other forms of illicit commerce. One significant concern is the link between terrorists seeking a WMD capability on the one hand and drug traffickers on the other.[57] A 2012 study of maritime trade patterns by the Stockholm International Peace Research Institute underscores this convergence.

Arms proliferation networks are increasingly adopting techniques pioneered by drug trafficking organizations that integrate their logistics operations within the global supply chain through the use of sealed shipping containers, which are carried aboard vessels that are owned by mainstream shipping companies and engaged in licit trade.

Hugh Griffiths and Michael Jenks
Maritime Transport and Destabilizing Commodity Flows
January 2012

Indeed, for the US and its neighbors, maritime flows could become a more important threat vector in the near term. As the US-Mexico border has become increasingly militarized, drug cartels at times have opted to avoid land routes and instead move their product in container ships transiting the Caribbean.[58] Another development that arguably is increasing the risk profile of maritime flows to the eastern US seaboard is the rise of "post-Panamax" vessels. The threat is not tied to the vessels themselves. Rather, since some US ports cannot accommodate the larger drafts, carriers employing such vessels are likely to increase calls at non-US transshipment ports that can meet requirements. In many cases, cargo at such transshipment points is offloaded onto smaller feeder vessels bound for the US.[59]

Protecting ports in major urban areas against infiltration by dangerous items, including WMDs, explosives, and biological and chemical agents is a top priority.[60] Although the primary concerns in this regard are inbound containers, dangerous materials also could be positioned to strike at major US port infrastructure by concealing them among conveyances of disparate items intended for export.[61] This is an overlooked area and one where proliferation, exporter compliance issues, and port security overlap.

However, shipping security is a far-reaching concern and is not limited to scenarios involving sensitive items. Along major shipping routes, and particularly at potential choke points in maritime traffic, including the Gulf of Aden (Bab el-Mandeb) and the Straits of Malacca, container ships are vulnerable to direct attack and piracy. While the Gulf of Guinea is not a major maritime bottleneck, attacks have been occurring there and have been targeted at oil tankers, with another vessel pulling up alongside the tanker and offloading the oil.[62]

Although international efforts have driven down the number of hijackings and hostage takings in the Gulf of Aden and Bab el-Mandeb, hijackings by Somali pirates continue to pose a threat, increasing operating costs as carriers hire private security firms to provide deterrence.[63] For example, in 2011, kidnap and ransom insurance for vessels crossing the Gulf of Aden cost $15,000-20,000 per transit for tankers, and $5,000-$10,000 for container ships.[64] However, many of these vessels are also outfitted

with security systems, including acoustic devises, razor wire, water cannon and, in some cases, security guards. The armed security guards apparently cost commercial shippers nearly $1 billion in 2012, about twice what they spent the prior year.[65]

Shipping is a dynamic industry, swayed by changes in the global economy, infrastructure development and climatic patterns. Likewise, threats to the shipping industry are not static, and the same forces that alter the legitimate supply chain influence their nature and prevalence.

Maritime shipping accounts for roughly 90 percent of global trade measured by volume. The main global shipping routes concentrate a large amount of traffic at a discrete number of strategic locations, such as the Straits of Malacca and Bab-el-Mandeb. Lax physical security, corruption and other weaknesses in these locales very directly raise potential for smuggling and piracy. Maritime traffic in the Gulf of Guinea, for example, is small compared to that of the Gulf of Aden or Straits of Malacca.[66]

Changes in demand at any point in global value chains can have cascading effects on shipping patterns. If Nigeria's volatile oil export market increases, or imports from West Africa continue to rise, maritime traffic — and the threat of piracy — will increase.[67] US imports predominantly come from South America, West Africa and the Middle East. However, with the US increasingly drawing on domestic energy sources, US interests will be less vulnerable to attacks in the Gulf of Aden and the Strait of Hormuz.

Shipping patterns are also influenced by infrastructure development and modernization projects, as well as climate changes. Current developments present an opportunity to address port security including trade controls and security at ports.

The expansion of the Panama Canal is forecast to have a major impact on maritime container shipping over the next decade, not least being a threefold increase in the size of vessels calling at some US ports. New challenges will arise as these larger ships enter certain US ports. Not all ports along the Gulf of Mexico and the East Coast, for example, have the capacity to accommodate larger vessels and increased traffic, which will lead to an increased commodity burden. Stakeholders have voiced their concern with the current infrastructure level.[68] With Panamax ships set to triple in size over the next few years, current infrastructure could come under major stress and amplify supply chain vulnerabilities.[69]

The Panama Canal expansion, in particular, is likely to increase demands on the US multimodal freight system. According to a recent report from the US Department of Transportation's Maritime Administration: "Terminals will need to increase the number of trucks they can efficiently handle each hour or each day by expanding physical gate facilities, speeding up processing through existing facilities (for example, with improved information technology and automation) and/or increasing their hours of operations."[70]

Efficiency will not be guaranteed by infrastructure expansion. It will also require better information flows across intermodal facilities. A World Trade Organization study on the efficiency of national border management systems ranks US import and export processing, respectively, as sixth and fifth worldwide.[71]

A 2013 Journal of Commerce study, however, reveals that the United States is lagging globally in terms of port and terminal productivity, affecting both export and imports.[72] Based on berth productivity, no US port is included in the global top ten most productive ports.[73] Already increased cargo shipments to US West Coast ports are slowed by a lack of coordination at truck transfer points.[74]

As industry takes advantage of increased traffic from Asia, it will want to ensure efficiency, looking to government to improve infrastructure at ports and intermodal points.

The US will also need to attract transshipment traffic. In response to the increased traffic through the Canal, ports throughout the Caribbean are vying to attract transshipment business on routes from Asia to Europe. The Port of Miami, which is now deepening its port to accommodate post-Panamax ship sizes, faces the challenge of ensuring an efficient transshipment process. [75]

Following 9/11, the port lost business when it began inspecting 100 percent of transshipment cargo.[76] Previously, transshipment had accounted for 20 percent of the port's business, but this dropped substantially as carriers opted for other Caribbean ports with less stringent regulations, such as Kingston and Freeport.[77] While the Port of Miami eventually made adjustments to offset some of these losses, it and other US ports will continue to face major challenges in adapting to current infrastructure trends and corresponding shifts in maritime traffic.

Changes in the climatic environment undoubtedly will influence shipping patterns, too. The opening of the Arctic seaway year-round will create a northern route from China to Rotterdam over Russia (the Northeast Passage[78]) or Canada (the Northwest Passage[79]), bypassing traditional bottlenecks such as the Panama Canal and the Straits of Malacca.

Increased commodity flows will only heighten the tension between security and efficiency. New shipping routes will open up new vulnerabilities, particularly to the extent they rely on transshipment ports without the operating standards or physical infrastructure for rigorous security. Customs and law enforcement agencies will be increasingly taxed as throughput increases. While these trends are daunting, they also can be embraced as an opportunity to enhance global supply chain security as well as commercial efficiency.

---

[1] This section is adapted from: Brian Finlay. "Minding Our Business: The Role of the Private Sector in Managing the WMD Supply Chain." *WMD Insights*. February 2009. Accessed November 20, 2013. http://www.hsdl.org/?view&did=38295.

[2] *Global Investment Trends Monitor,* No. 15. Geneva: United Nations Conference on Trade and Development (UNCTAD), 2014). Accessed February 3, 2014. http://unctad.org/en/PublicationsLibrary/webdiaeia2014d1_en.pdf.

[3] Stulberg, Adam N. and Matthew Fuhrmann, eds. *The Nuclear Renaissance and International Security*. Redwood City: Stanford University Press, 2013.

[4] Fitzpatrick, Mark, ed. "Nuclear Black Markets: Other Countries and Networks." In *Nuclear Black Markets: Pakistan, A.Q. Khan and the Rise of Proliferation Networks — A Net Assessment,* 43-64. London: International Institute for Strategic Studies, 2007.

[5] National Research Council. *Globalization, Biosecurity, and the Future of the Life Sciences*. Washington, DC: National Academies Press, 2006; Bhattacharya, Sujit, and Jayanthi A. Pushkaran Shilpa. *Nanotechnology Development in India: Investigating Ten Years of India's Efforts in Capacity Building*. New Delhi: CSIR-National Institute of Science Technology and Development Studies, 2012. Accessed February 4, 2014. http://www.nistads.res.in/images/recentupd/BriefingpaperI_Website.pdf.

[6] Naim, Moisés. *Illicit: How Smugglers, Traffickers and Copycats are Hijacking the Global Economy*. New York: Doubleday, 2005; Luna, David M. "The Destructive Impact of Illicit Trade and the Illegal Economy on

Economic Growth, Sustainable Development, and Global Security." Remarks delivered at the OECD High-Level Risk Forum, Paris, France, October 26, 2012. US Department of State (DoS). Bureau of International Narcotics and Law Enforcement Affairs. Accessed February 3, 2014. http://www.state.gov/j/inl/rls/rm/199808.htm.

[7] US Library of Congress (LoC). Congressional Research Service (CRS). *The United Arab Emirates (UAE): Issues for U.S. Policy.* By Katzman, Kenneth. February 2014. Accessed February 26, 2014. http://www.fas.org/sgp/crs/mideast/RS21852.pdf.

[8] The UN has increased its focus on measuring these important economic activities. Further information can be found at United Nations Statistics Division. "Statistics of International Trade in Services and Tourism." United Nations Statistics Division Trade Statistics Branch. http://unstats.un.org/unsd/tradeserv/default.htm. For background on international trade in services, see Coalition of Services Industries. "The Trade in Services Agreement." Coalition of Services Industries Trade Negotiations. https://servicescoalition.org/negotiations/trade-in-services-agreement.

[9] Office of the United States Trade Representative (USTR). "US-Canada Trade Facts." Office of the United States Trade Representative Resource Center. Accessed April 1, 2014. http://www.ustr.gov/countries-regions/americas/canada.

[10] USTR. "European Union." Office of the United States Trade Representative Resource Center. Accessed April 1, 2014. http://www.ustr.gov/countries-regions/europe-middle-east/europe/european-union. This excludes trade in military services and other miscellaneous government services, according to the US Trade Representative.

[11] US Department of Justice (DoJ). *Summary of Major US Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases*. March 2014. Accessed April 2, 2014. http://pmddtc.state.gov/compliance/documents/OngoingExportCaseFactSheet012014.pdf.

[12] Picard, Justin. "Can We Estimate the Global Scale and Impact of Illicit Trade." In *Convergence*, edited by Michael Miklaucic and Jacqueline Brewer, 52. Washington, DC: National Defense University Press, 2013.

[13] Ibid., 57.

[14] Ibid., 52.

[15] Ibid., 54.

[16] Parrish, Karen. "Link Grows Between Terrorism, Organized Crime, Officials Say." American Forces Press Service, March 28, 2012. Accessed May 6, 2013. http://www.defense.gov/news/newsarticle.aspx?id=67721.

[17] Farah, Douglas. "Fixers, Super Fixers, and Shadow Facilitators: How Networks Connect." In *Convergence*, edited by Michael Miklaucic and Jacqueline Brewer, 75-98. Washington, DC: National Defense University Press, 2013; Lormel, Dennis M. "Assessing the Convergence between Terrorist Groups and Transnational Criminal Organizations." ACAMS Today, March 6, 2014. Accessed March 10, 2014. http://acamstoday.org/wordpress/2014/03/06/assessing-convergence-terrorist-groups-transnational-criminal-organizations/.

[18] DoS. Bureau of Counterterrorism. *Country Reports on Terrorism 2011*. July 2012. Accessed June 6, 2013. http://www.state.gov/j/ct/rls/crt/2011/195549.htm; http://www.ict.org.il/NewsCommentaries/Commentaries/tabid/69/Articlsid/892/currentpage/10/Default.aspx

[19] Nuclear Threat Initiative. "Argentina Overview." Nuclear Threat Initiative Country Profiles. Last modified February 2014. Accessed March 5, 2014. http://www.nti.org/country-profiles/argentina/; Nuclear Threat

Initiative. "Brazil Overview." Nuclear Threat Initiative Country Profiles. Last Modified February 2014. Accessed March 5, 2014. http://www.nti.org/country-profiles/brazil/.

[20] United States v. Ayman Joumaa. 1:11-CR-560 (ED Virginia. 2011). Accessed February 5, 2014. http://www.investigativeproject.org/documents/case_docs/1856.pdf; Hernández, Joel. "Terrorism, Drug Trafficking, and the Globalization of Supply." *Perspectives on Terrorism* 7, no. 4 (August 2013): 41-61. Accessed November 5, 2013. http://www.terrorismanalysts.com/pt/index.php/pot/article/view/281/html.

[21] Testimony of Celina Realuyo and Douglas Farah, US Congress. House. *Terrorist Groups in Latin America: The Changing Landscape.* 113th Cong., 2d sess., February 4, 2014.

[22] Kan, Paul Rexton, Bruce E. Bechtol Jr., and Robert M. Collins. *Criminal Sovereignty: Understanding North Korea's Illicit International Activities.* Carlisle, PA: Strategic Studies Institute, US Army War College, 2010. Accessed February 7, 2013. http://www.dtic.mil/dtic/tr/fulltext/u2/a518777.pdf.

[23] LoC. CRS. *Drug Trafficking and North Korea: Issues for U.S. Policy*. By Perl, Raphael F. January 2007. Accessed February 5, 2013. https://www.fas.org/sgp/crs/row/RL32167.pdf.

[24] Kan, Paul Rexton, Bruce E. Bechtol Jr., and Robert M. Collins. *Criminal Sovereignty: Understanding North Korea's Illicit International Activities*. Carlisle, PA: Strategic Studies Institute, US Army War College, 2010. Accessed February 7, 2013. http://www.dtic.mil/dtic/tr/fulltext/u2/a518777.pdf.

[25] Kilcarr, Sean. "Cargo Thieves Becoming 'Strategists,' Say Experts." FleetOwner, August 9, 2013. Accessed September 23, 2013. http://fleetowner.com/fleet-management/cargo-thieves-becoming-strategists-say-experts; Mello Jr., John P. "Target Fiasco Shines Light on Supply Chain Attacks." TechNewsWorld, February 3, 2014. Accessed February 4, 2014. http://www.technewsworld.com/story/79908.html; Dowdy, John. "The Cybersecurity Threat to U.S. Growth and Prosperity." In *Securing Cyberspace: A New Domain for National Security*, by Nicholas Burns and Johnathon Price, 129-143. Washington, DC: The Aspen Institute, 2012; Dunn, John E. "Hackers Planted Remote Devices to Smuggle Reports Through Antwerp Port, Europol Reveals." TechWorld, October 16, 2013. Accessed October 21, 2013. http://news.techworld.com/security/3474018/hackers-planted-remote-devices-to-smuggle-drugs-through-antwerp-port-europol-reveals.

[26] Kramek, Joseph. *The Critical Infrastructure Gap: US Port Facilities and Cyber Vulnerabilities*. Washington, DC: Brookings Institution, 2013. Accessed November 7, 2013. http://www.brookings.edu/research/papers/2013/07/03-cyber-ports-security-kramek; "UT Austin Researchers Spoof Superyacht at Sea." University of Texas at Austin Cockrell School of Engineering, July 29, 2013. Accessed November 7, 2013. http://www.engr.utexas.edu/features/superyacht-gps-spoofing.

[27] "'Pirate Trails' Tracks Dirty Money Resulting from Piracy Off the Horn of Africa." The World Bank, November 1, 2013. Accessed November 12, 2013. http://www.worldbank.org/en/news/press-release/2013/11/01/pirate-trails-tracks-dirty-money-resulting-from-piracy-off-the-horn-of-africa; Kirkpatrick, David D. "SEAL Team Raids a Tanker and Thwarts a Militia's Bid to Sell Libyan Oil." New York Times, March 17, 2014. Accessed April 8, 2014. http://www.nytimes.com/2014/03/18/world/middleeast/libya-oil-tanker.html; "Report Highlights Rise of Maritime Crime in Southeast Asia." MarineLink.com, March 15, 2013. Accessed October 16, 2013. http://www.marinelink.com/news/highlights-maritime352582.aspx; "Trouble for US Importers and CBP: Importer Identity Theft." CustomsNow, June 29, 2010. Accessed September 19, 2013. http://www.customsnow.com/blog/2010/06/trouble-for-us-importers-and-cbp-importer-identity-theft/; Interview with industry by author. Washington, DC. January 10, 2014.

[28] Bailes, Alyson JK. "Terrorism and Business." Statement made at the Groupe d'Economie Mondiale, Sciences-Po, Paris, September 5, 2006. Accessed February 4, 2014. http://www.gem.sciencespo.fr/content/news_events/pdf/bailes_Terror050906.pdf.

[29] Testimony of Celina Realuyo and Douglas Farah, US Congress. House. *Terrorist Groups in Latin America: The Changing Landscape*. 113th Cong., 2d sess., February 4, 2014.

[30] Brühl, Jannis. "Where did Syria's Chemical Weapons Come From?" ProPublica, September 25, 2013. Accessed October 3, 2013. http://www.propublica.org/article/where-did-syrias-chemical-weapons-come-from.

[31] Chestnut, Sheena. "Illicit Activity and Proliferation: North Korean Smuggling Networks." *International Security* 32, no. 1 (Summer 2007): 80-111.

[32] Germain, Timothée. "Corée du Nord : Cartographie de la prolifération." *Observatoire de la Non-Prolifération*, no. 73 (December 2012). Accessed January 29, 2014. http://www.cesim.fr/observatoire/fr/73/article/87.

[33] Albright, David, and Christina Walrond. *Iran's Critical Capability in 2014: Verifiably Stopping Iran from Increasing the Number and Quality of its Centrifuges*. Washington, DC: Institute for Science and International Security, 2013. Accessed January 29, 2014. http://isis-online.org/uploads/isis-reports/documents/Iran_critical_capability_17July2013.pdf; Albright, David. *Ring Magnets for IR-1 Centrifuges*. Washington, DC: Institute for Science and International Security, 2013. Accessed January 29, 2014. http://isis-online.org/uploads/isis-reports/documents/iran_ring_magnet_13Feb2013.pdf; DoJ. Office of Public Affairs. *Two Indicted for Alleged Efforts to Supply Iran with U.S.-Materials for Gas Centrifuges to Enrich Uranium*. July 2012. Accessed January 29, 2014. http://www.justice.gov/opa/pr/2012/July/12-nsd-873.html.

[34] US Department of Commerce (DOC). Bureau of Industry and Security (BIS). *Don't Let This Happen to You: An Introduction to US Export Control Law*. September 2010. Accessed August 25, 2013. https://www.bis.doc.gov/index.php/forms-documents/doc_download/535-don-t-let-this-happen-to-you-2010.

[35] For an overview, see World Nuclear Association. "Radioisotopes in Medicine." Radioisotopes and Research. Non-Power Nuclear Applications. Information Library. Last modified July 2014. Accessed August 11, 2014. http://www.world-nuclear.org/info/Non-Power-Nuclear-Applications/Radioisotopes/Radioisotopes-in-Medicine/.

[36] International Physicians for the Prevention of Nuclear War (IPPNW). "ICAN: Highly enriched uranium (HEU) in radiopharmaceutical production." The International Campaign to Abolish Nuclear Weapons (ICAN). Abolition of Nuclear Weapons. Accessed April 4, 2014. http://www.ippnw.org/ican/heu.html.

[37] Nilsen, Ashley. "The New Face of Illicit Trafficking Networks," Presentation at the Pacific Northwest International Conference on Global Security - The Decade Ahead, Portland, Oregon, 2011.

[38] Farah, Douglas. "Fixers, Super Fixers, and Shadow Facilitators: How Networks Connect." In *Convergence*, edited by Michael Miklaucic and Jacqueline Brewer, 75-98. Washington, DC: National Defense University Press, 2013: 75-98.

[39] DoJ. *Summary of Major US Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases*. March 2014. Accessed April 2, 2014. http://pmddtc.state.gov/compliance/documents/OngoingExportCaseFactSheet012014.pdf.

[40] DoJ. *Summary of Major US Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases*. March 2014. Accessed April 2, 2014. http://pmddtc.state.gov/compliance/documents/OngoingExportCaseFactSheet012014.pdf. 62.

[41] DOC. BIS. *Budget Estimates, Fiscal Year 2014*. March 2013. Accessed April 29, 2014. http://www.osec.doc.gov/bmi/budget/FY14CJ/BIS_FY_2014_CJ_Final_508_Compliant.pdf. 56.

[42] For information on the future direction of the FATF, see Nechaev, Vladimir. "The Role of the Asia/Pacific Group on Money Laundering in the Global AML/CFT Network." Keynote address at the 16th annual meeting of the Asia Pacific Group on Money Laundering (APG), Shanghai, July 16, 2013. Accessed September 26, 2013. http://www.fatf-gafi.org/documents/news/apg-keynote-address-2013.html.

[43] Financial Crimes Enforcement Network. "Home." Accessed August 8, 2013. http://www.fincen.gov/.

[44] DoJ. *Summary of Major US Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases*. March 2014. Accessed April 2, 2014. http://pmddtc.state.gov/compliance/documents/OngoingExportCaseFactSheet012014.pdf; Wall, J.K. "Lilly Scientists Stole $55 Million in Trade Secrets, Indictment Alleges." International Business Journal News, October 8, 2013. Accessed October 21, 2013. http://www.ibj.com/lilly-employees-stole-55-million-in-trade-secrets-indictment-alleges/PARAMS/article/43949.

[45] Butler, Declan. "Viral Research Faces Clampdown." Nature, October 23, 2012. Accessed September 19, 2013. http://www.nature.com/news/viral-research-faces-clampdown-1.11629; Maher, Brendan. "Bird-Flu Research: The Biosecurity Oversight." Nature, May 23, 2012. Accessed October 3, 2013. http://www.nature.com/news/bird-flu-research-the-biosecurity-oversight-1.10695.

[46] Author interview; See US Executive Office of the President (EOP). *Administration Strategy on Mitigating the Theft of US Trade Secrets*. February 2013. Accessed August 13, 2013. http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf; and FBI efforts to address intellectual property theft http://www.fbi.gov/about-us/investigate/white_collar/ipr/ipr.

[47] Gruselle, Bruno. *Proliferation Networks and Financing*. Paris: Fondation Pour la Recherché Stratégique, 2007. Accessed January 30, 2014. http://www.frstrategie.org/barreFRS/publications/rd/RD_20070303_eng.pdf; DoJ. Office of Public Affairs. *Belgian Man Charged with Attempting to Illegally Export Aluminum Tubes to Malaysian Front for Individual in Iran*. October 2013. Accessed January 31, 2014. http://www.justice.gov/usao/iln/pr/chicago/2013/pr1030_01.html.

[48] Wirtz, Ralf. "Finding Innovative Ways to Detect and Thwart Illicit Nuclear Trade." Remarks made at the Carnegie Nonproliferation Conference, Washington, DC, June 26, 2007. Accessed January 26, 2014. http://www.carnegieendowment.org/files/detect_thwart.pdf; Albright, David and Corey Hinderstein. *Creation of Leybold's Internal Compliance System*. Washington, DC: Institute for Science and International Security, 2002. Accessed January 29, 2014. http://isis-online.org/conferences/detail/creation-of-leybolds-internal-compliance-system/20.

[49] Albright, David. "The Leybold Charter: Putting Non-Proliferation Above Commercial Interests." In *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies*. New York: Free Press, 2010.

[50] Letter from Assistant Secretary of State Paul V. Kelly to Senator Russ Feingold. June 2, 2004.

[51] Farah, Douglas, and Stephen Braun. Merchant of Death: Money, Guns, Planes, and the Man Who Makes War Possible. Hoboken, NJ: Wiley, 2007.

[52] Stempel, Jonathan. "Russian Arms Dealer Viktor Bout's US Conviction Upheld." Reuters, September 27, 2013. Accessed October 2, 2013. http://www.reuters.com/article/2013/09/27/us-usa-crime-bout-idUSBRE98Q0PG20130927.

[53] Moran, Matthew and Daniel Salisbury. *Sanctions and the Insurance Industry: Challenges and Opportunities*. London: King's College Centre for Science & Security Studies, 2013. http://www.kcl.ac.uk/sspp/departments/warstudies/research/groups/csss/pubs/insurancereport.pdf.

[54] The Standard Club. "The Club." Accessed September 13, 2013. http://www.standard-club.com/who-we-are/the-club/.

[55] Lister, Tim. "Syrian-Bound Russian Cargo Ship Loses Insurance." CNN, June 19, 2012. Accessed August 30, 2013. http://www.cnn.com/2012/06/18/world/meast/syria-cargo-ship/; Saul, Jonathan, and Thomas Grove. "Russia Syria-Bound Arms Ship Turns Back: Britain." Reuters, June 19, 2012." Accessed August 30, 2013. http://www.reuters.com/article/2012/06/19/us-syria-weapons-ship-idUSBRE85I0Q520120619; Black, Ian, and Severin Carrell. "Russian Arms Shipment Bound for Syria Foiled by Britain's Insurers." The Guardian, June 19, 2012. Accessed August 30, 2013. http://www.theguardian.com/world/2012/jun/19/syria-arms-shipment-foiled.

[56] DoJ. *Summary of Major US Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases*. March 2014. Accessed April 2, 2014. http://pmddtc.state.gov/compliance/documents/OngoingExportCaseFactSheet012014.pdf.

[57] Hernández, Joel. "Terrorism, Drug Trafficking, and the Globalization of Supply." *Perspectives on Terrorism* 7, no. 4 (August 2013): 41–61. Accessed November 5, 2013. http://www.terrorismanalysts.com/pt/index.php/pot/article/view/281/html.

[58] Fieser, Ezra. "Sinaloa Cartel Carves Drug Routes in the Caribbean." *Global Post*, February 18, 2012. Accessed December 17, 2013. http://www.globalpost.com/dispatch/news/regions/americas/120217/sinaloa-cartel-drug-routes-drug-war-cocaine-caribbean.

[59] Krayewski, Ed. "Panama Canal Expansion Fueling Port Upgrades; Some US Ports Burdened by Security, Environmental Regulations." Reason.com, November 29, 2012. Accessed December 11, 2013. http://reason.com/blog/2012/11/29/panama-canal-expansion-fueling-port-expa; *US Port and Inland Waterways Modernization: Preparing for Post-Panamax Vessels.* Washington, DC: Institute for Water Resources, US Army Corps of Engineers, June 20, 2012. Accessed November 15, 2013.http://www.iwr.usace.army.mil/Portals/70/docs/portswaterways/rpt/June_20_U.S._Port_and_Inland_Waterways_Preparing_for_Post_Panamax_Vessels.pdf.

[60] Maney, Kevin P. "'Said to Contain': Fear of Incurring Liability Creates a Disincentive for Cargo Carriers to Improve Shipping Container Security by Examining Cargo." *Tulane Maritime Law Journal* 35, no.1 (Winter 2010): 318.

[61] In 2012, the assistant director of the Port of San Diego remarked: "Our… mission is to protect the American homeland against terrorists and from weapons of mass effect from entering the country… Given the waterways and the access to the Navy fleet here, I'd say, absolutely, San Diego is a target." IPT News. "Port Official's WMD Comment Stirs Concerns." The Investigative Project on Terrorism Blog, February 14, 2011. Accessed November 16, 2013. http://www.investigativeproject.org/2594/port-official-comment-wmd-stirs-concerns.

[62] Barrios, Cristina. "Fighting Piracy in the Gulf of Guinea." European Union Institute for Security Studies, Issue Brief no. 20 (May 2013): 1. Accessed December 12, 2013. http://www.iss.europa.eu/uploads/media/Brief_20.pdf.

[63] Rayman, Noah. "Did 2013 Mark the End of Somali Piracy?" *Time*, January 6, 2014. Accessed January 31, 2014. http://world.time.com/2014/01/06/did-2013-mark-the-end-of-somali-piracy/; DoS. Bureau of Political-Military Affairs. *Contact Group on Piracy off the Coast of Somalia: Quarterly Update: Fact Sheet*. December 24, 2013. Accessed January 30, 2014. http://www.state.gov/t/pm/rls/fs/2013/219088.htm.

[64] *The Economic Cost of Somali Piracy, 2011.* Broomfield, CO*:* One Earth Future Foundation, 2011. Accessed April 27, 2014. http://oceansbeyondpiracy.org/sites/default/files/economic_cost_of_piracy_2011.pdf. 16.

[65] Pinksker, Joe. "The Pirate Economy." The Atlantic, April 16, 2014. Accessed May 9, 2014. http://www.theatlantic.com/magazine/archive/2014/05/the-pirate-economy/359817/.

[66] Kang, Harnit Kaur. "Gulf of Aden vs Malacca Strait: Piracy and Counter-piracy Efforts." Institute of Peace and Conflict Studies, Issue Brief no. 135 (December 2009): 1-4. Accessed December 11, 2013. http://www.ipcs.org/pdf_file/issue/IB135-SEARP-Harnit1.pdf.

[67] Vollgraaff, Rene. "Nigerian Economy Expands 6.81% in Third Quarter on Oil." Bloomberg News, November 18, 2013. Accessed December 9, 2013. http://www.bloomberg.com/news/2013-11-18/nigerian-economy-expands-6-81-in-third-quarter-on-oil.html.

[68] US Department of Transportation (DOT). Bureau of Transportation Statistics. "Table 1-2: Number of Air Carriers, Railroads, Interstate Motor Carriers, Marine Vessel Operators, and Pipeline Operators." Accessed January 29, 2014. http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/html/table_01_02.html_mfd.

[69] Cuadra, Alberto, Gene Thorp, and Bill Webster. "Modernization of the Panama Canal." *Washington Post*, January 13, 2013. Accessed December 5, 2013. http://www.washingtonpost.com/wp-srv/special/world/modernization-of-panama-canal/.

[70] "Study Finds Panama Canal Expansion Will Affect U.S. Trucking." Truckinginfo, December 4, 2013. Accessed December 10, 2013. http://www.truckinginfo.com/news/story/2013/12/study-finds-panama-canal-expansion-will-affect-u-s-trucking.aspx.

[71] Doing Business Project. "Trading Across Borders." Doing Business Project Data Topics. Last modified June 2013. Accessed January 30, 2014. http://www.doingbusiness.org/data/exploretopics/trading-across-borders; Mongelluzzo, Bill. "Bigger Ships and Righter Supply Chains Shine a New Light on Port Productivity and its Importance to Shippers." In *Key Findings on Terminal Productivity Performance Across Ports, Countries and Regions.* Newark, NJ: The Journal of Commerce Group Inc., 2013. Accessed January 30, 2014. http://www.portoflosangeles.org/Board/2013/September%202013/091913_Agenda_Audit_Committee_Item_3.pdf.

[72] Mongelluzzo, Bill. "Terminal Velocity." Journal of Commerce, July 22, 2013. Accessed January 31, 2014. http://www.apmterminals.com/uploadedFiles/corporate/Media_Center/In_The_News/APM%20Terminals%20Terminal%20Velocity%20article.pdf.

[73] Ibid.

[74] Bonney, Joseph. "US Ports Shift Focus to Operational Efficiency." Journal of Commerce, January 7, 2014. Accessed January 9, 2014. http://www.joc.com/port-news/port-productivity/us-ports-shift-focus-operational-efficiency_20140107.html.

[75] "USA: Port of Miami — Up to the Challenge in 2014." DredgingToday.com, October 5, 2010. Accessed December 2, 2013. http://www.dredgingtoday.com/2010/10/05/usa-port-of-miami-up-to-the-challenge-in-2014/.

[76] Diaz, Jennifer. "PortMiami and CBP Join Forces to Bring Back (and Expedite) Transshipment." Customs and International Trade Law Blog, November 19, 2013. Accessed December 10, 2013. http://www.customsandinternationaltradelaw.com/2013/11/articles/import/portmiami-and-cbp-join-forces-to-bring-back-transshipment/.

[77] Miami-Dade County. Dante B. Fascell Port of Miami. *PortMiami Focuses on Transshipment Business — Form Committee*." November 2013. Accessed December 10, 2013. http://www.miamidade.gov/portmiami/press_releases/2013-11-19-transshipment-business.asp.

[78] Shell, Elizabeth. "China May Have New Shipping Shortcut Thanks to Melting Arctic Ice." PBS, August 20, 2013. Accessed December 10, 2013. http://www.pbs.org/newshour/rundown/2013/08/china-has-a-new-short-cut-thanks-to-melting-arctic-ice.html.

[79] "Short and Sharp." The Economist, June 16, 2012. Accessed December 10, 2013. http://www.economist.com/node/21556803.

International Trade Controls

MULTILATERAL EXPORT CONTROL REGIMES

Trade liberalization has prompted efforts to mitigate a commensurate rise in illicit commerce, particularly in dangerous materials and sophisticated technologies.[80] These efforts are embodied in the major multilateral export control regimes.

At various times, these efforts have been driven by individual countries, groups of countries, the United Nations or civil society actors. All arrangements are voluntary and subject to national laws and regulations. The US export control regime operates within the context of this international system of controls.

Major Multilateral Export Control Regimes

Regime	Year Established	Number of Current Members	Items Covered	Notable Non-Member Countries
The Zangger Committee	1971	38	Nuclear Supplies	India, Iran, Israel, North Korea, Pakistan, Syria
The Nuclear Suppliers Group	1974	46	Nuclear Weapons	India, Iran, Israel, North Korea, Pakistan, Syria
The Australia Group	1985	42	Biological and Chemical Weapons	China, India, Iran, Israel, North Korea Pakistan, Russia, Syria, South Africa
Wassenaar Agreement	1995	41	Conventional Arms and Dual-Use Items	China, India, Iran, Israel, North Korea, Pakistan, Syria
Missile Technology Control Regime	1987	34	Missiles	China, India, Iran, Israel, North Korea Pakistan, Syria

A brief history of each of these regimes follows.

THE ZANGGER COMMITTEE (NUCLEAR SUPPLIES)

The Zangger Committee began as an informal meeting among representatives from several States Parties to the Nuclear Nonproliferation Treaty (NPT), along with those of several other states. The group had held a series of meetings in Vienna in 1971 and 1974 to define "equipment or material especially designed or prepared for the processing, use or production of special fissionable material," as well as the conditions and procedures that would govern exports of equipment and material in order to better meet the requirements of article III, paragraph 2 of the NPT. These meetings occurred with the understanding that Committee participants would not be legally bound by their result. The Zangger Committee ultimately reached consensus on the following "understandings" regarding nuclear material and associated equipment:

- Nuclear material transferred to non-nuclear weapons states must not be diverted for use in nuclear weapons.
- Nuclear material and associated equipment transferred to non-nuclear weapons states must be subject to IAEA safeguards.
- Such material and equipment may not be re-exported to another non-nuclear weapons state unless the recipient adheres to IAEA safeguards.[81]

The member states also created a "trigger list," a compilation of which items were triggers of IAEA safeguards. This list was published as IAEA document INFCIRC/209 in 1974 and since then has been amended six times: in 1977, 1984, 1985, 1990, 1994 and 1996. In 1994, the list was revised to better clarify materials utilized in the enrichment process as well as equipment utilized in the primary cooling process. The Committee has no body or system of verification as its membership is voluntary, but it meets twice a year in an informal setting. Most recently, the Chairman hosted a background briefing of the Committee's work at the 2012 NPT Preparatory Committee meeting and the Committee participated in and became a permanent observer of the 23rd Plenary Meeting of the Nuclear Suppliers Group (NSG) in 2013.

The Zangger Committee currently has 38 members.

THE NUCLEAR SUPPLIERS GROUP (NUCLEAR WEAPONS)

The Nuclear Suppliers Group (NSG) was established after the 1974 explosion of a nuclear device by India, a non-nuclear-weapon state. The IAEA published the NSG's Guidelines in 1978 as IAEA Document INFCIR/254.[82] The Guidelines were to be applied to nuclear transfers for peaceful purposes. Their goal was to ensure that nuclear technology that had been transferred for peaceful purposes would not be weaponized or otherwise misused. In 1990, the Nonproliferation Treaty (NPT) Review Conference made several recommendations that shaped NSG activity in the 1990s. Until 1992, the NSG operated without guidelines for transfers of nuclear-related dual-use materials. Part 1 of the NSG was updated in June 2012, Part 2 in August 2012.

Creation of Part 1 of the NSG included the consideration of the Zangger Committee trigger list.[83] The two lists vary in their areas of focus. The Zangger list is confined to items falling under Article III.2 of the NPT, while the NSG has a formal scope of safeguards that accompany

the trigger list.[84] The NSG also advocates best practices regarding customer vetting, information sharing, and industry participation in non-proliferation efforts.[85]

There are clear similarities between the missions of the Zangger Committee and the NSG. The NSG builds upon the Zangger Committee's standards, and is more robust in scope and in its public reporting mechanisms. Although there has been discussion of merging the Zangger Committee and the NSG, they will likely remain separate to allow suppliers discrete membership options.[86]

The NSG currently has 46 members.

THE AUSTRALIA GROUP (CHEMICAL AND BIOLOGICAL WEAPONS)

After Iraq violated the 1925 Geneva Protocol by using chemical weapons during the Iran-Iraq war, numerous countries introduced export controls to prevent the movement of chemical precursors and materials that could be used in the production of such weapons. These controls were not universal, and efforts to evade them prompted Australia to propose a meeting of those countries with export controls.

In the summer of 1985, 15 countries and the European Commission met in Brussels to discuss methods to universalize the various export controls employed by different countries. States have since met every year and membership has expanded to 42 countries and the European Commission. New members are admitted by consensus of the Group, which most recently added Mexico to its ranks in June 2013. The control lists of the group have expanded from precursors and materials to include technology and equipment that can be used both in the production and disposal of chemical and biological weapons.[87] The states seek to combat the proliferation of biological and chemical weapons, materials and technology, and contribute to information sharing to harmonize transfer controls.[88]

The Australia Group is an informal and voluntary group with no regulating body. However, each member nation is charged with adhering to the Group's objectives, goals and recommendations. All Group participants are also members of the Chemical Weapons Convention (CWC) and the Biological Weapons Convention (BWC) and agreed that the Group would be a "practical way to uphold the core purpose of these accords: preventing the spread of chemical and biological weapons."[89]

In June 2002, members agreed to a set of formal but non-binding criteria for export requests. These guidelines include a disavowal of "undercutting" and a pledge not to institute "catch-all" controls. The "no undercutting" provision does not allow countries to grant the exportation of materials which other countries have previously denied permission to export. Additionally, this provision requires that countries halt the exportation of any substance that could be used in the importer's production of chemical or biological weapons (CBW), whether or not it appears on the Group's control lists. This requirement also requires that exporters notify their respective governments if they suspect importers of CBW manufacturing, research or development. In June 2002, the Group also agreed to prohibit transmission of CBW technologies via email, phone or fax.[90]

The five categories of the Australia Group's control lists are:

- Chemical weapons precursors
- Dual-use chemical manufacturing facilities, equipment and related technology
- Biological agents
- Toxins
- Dual-use biological equipment[91]

The Australia Group currently has 42 members.

THE WASSENAAR ARRANGEMENT (CONVENTIONAL ARMS AND DUAL-USE ITEMS)

The Wassenaar Arrangement was a crucial adjustment in post-Cold War relations. From 1950 until 1994, the multilateral Coordinating Committee for Multilateral Export Controls (COCOM) harmonized the efforts of the United States and its allies to limit the export of strategic materials and technologies to the countries of the Warsaw Pact. As East versus West tensions abated in the early 1990s, Western countries came to view COCOM as an anachronism. In 1993, member states agreed to eliminate COCOM and replace it with a new multilateral export control regime.[92] Participating states worked toward developing new goals, rules and procedures and to develop new lists of goods and technologies that would be continually updated and controlled. The Russian Federation, the Czech Republic, Poland and the Slovak Republic were among the founding group of the Wassenaar Arrangement in December 1995.

The Arrangement is a voluntary international agreement that seeks to "promote transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations."[93] Using best practices outlined by the Arrangement for export and transfer, Wassenaar members agree to institute national policy that ensures the responsible transfer of conventional weapons and dual-use items, as well as to "report on transfers and denials of specified controlled items to destinations outside the Arrangement."[94] Members also agree to control and prevent unauthorized transfers or re-transfers"[95] of all items that fall under the agreement's two control lists: Dual-Use and Munitions, which are divided into "basic," "sensitive," and "very sensitive." Munitions deliveries and "basic" dual-use weaponry must both be reported every six months.

Although the Arrangement's objective is to prevent countries or regions from obtaining "destabilizing accumulations" or huge stockpiles of weapons of "sensitive materials," no countries are specified in the Arrangement.[96] Although Arrangement decisions generally have come by consensus, Russia's policy diverged in 2000 when it announced it would resume sales to Iran. Friction among Arrangement members has also resulted from contravention of other members' previous denials, referred to as "undercutting." The Arrangement does not prohibit undercutting, although it does require participants to notify other participants within 60 (preferably 30) days when approving an export transaction that previously had been denied by other participants.

The Wassenaar Arrangement currently has 41 adherents.

The Missile Technology Control Regime

The G-7 countries (Canada, France, Germany, Italy, Japan, the UK, and the United States) established the Missile Technology Control Regime (MTCR) in 1987.[97] The MTCR is "an informal and voluntary association of countries which share the goals of non-proliferation of unmanned delivery systems capable of delivering weapons of mass destruction, and which seek to coordinate national export licensing efforts aimed at preventing their proliferation."[98] Originally established to prevent the spread of nuclear-weapon delivery systems, the Regime extended its focus in 1992 to missiles for the delivery of chemical and biological weapons as well.[99]

The MTCR organizes missile technology into two categories. [100] Category I includes those items that can carry a 500 kilogram payload over 300 kilometers. Category I items are rarely authorized for export and must overcome a strong presumption of denial.[101] Category II technology is permitted for export and includes "complete rocket systems…not covered in item I, capable of a maximum range equal to or greater than, 300km" as well as a wide range of materials, equipment and technologies used in UAVs.[102] Category II items require a review and licensing process through government agencies.

Under the MTCR, exporters of Category I and II items must consider the following in their decision making:

- the potential for WMD proliferation
- the objectives and capabilities of the recipient
- the relative significance of the technology to the recipient's potential development of WMD delivery systems
- the nature and credibility of recipient's assured end use
- the applicability of other multilateral agreements to the transfer
- the risk of diversion to terrorists or other malevolent non-state actors

The MTCR currently has 34 members.

United Nations Initiatives

Security Council Resolution 1540

In 2004, the United Nations Security Council adopted Resolution 1540 (UNSCR 1540), committing UN member states to combat the proliferation of nuclear, chemical, and biological weapons and their delivery mechanisms. The resolution further obliges states to "refrain from supporting by any means non-State actors from developing, acquiring, manufacturing, possessing, transporting, transferring or using nuclear, chemical or biological weapons and their

delivery systems."[103] Resolutions 1673 (2006), 1810 (2008) and 1977 (2011) extended the commitments of Resolution 1540 for two years, three years and until 2021 respectively.[104] The primary obligation of UNSCR 1540 is the criminalization of the acquisition, possession, development, transport, transference of WMDs and their means of delivery and associated materials, and to provide for accounting and security surrounding such items, as well as to ensure related border and export controls.[105]

TARGETED SANCTIONS REGIMES

Under Chapter VII of the UN Charter, the Security Council may impose mandatory sanctions on countries or groups of countries in the interest of international peace and security. Since 1992, the Security Council has issued 16 sanctions resolutions affecting 14 regions or countries where peace has been threatened and diplomatic efforts have been unsuccessful. These sanctions can target individuals as well as political or other entities and typically involve economic, visa and other measures.

Over time, the Security Council has refined its approach to target individuals or entities determined to be responsible for crises and to design "smart sanctions" that are triggered by specific events. Each sanctions regime is overseen by a special committee responsible for its implementation.[106] When a committee concludes that it has completed its work or that the conditions justifying the sanctions have ceased to exist, the Security Council can pass a separate resolution terminating the committee. Thirteen sanctions committees have been terminated in this manner.[107]

Currently active sanctions committees are listed below in chronological order of their enabling Security Council resolutions:[108]

- *Somalia and Eritrea* – Resolutions 751 (1992) and 1907 (2009)
- *Al-Qaeda and associated individuals and entities* – Resolutions 1267 (1999) and 1989 (2011)
- *Iraq* – Resolution 1518 (2003)
- *Liberia* – Resolution 1521 (2003)
- *Democratic Republic of the Congo* – Resolution 1533 (2004)
- *Côte d'Ivoire* – Resolution 1572 (2004)
- *Sudan* – Resolution 1591 (2005)
- *Beirut bombing* – Resolution 1636 (2006)
- *Democratic People's Republic of Korea* – Resolution 1718 (2006)
- *Islamic Republic of Iran* – Resolution 1737 (2006)
- *Libya* – Resolution 1970 (2011)
- *Taliban* – Resolution 1988 (2011)
- *Guinea-Bissau* – Resolution 2048 (2012)
- *Central African Republic* – Resolution 2127 (2013)

Committees Dealing with Terrorism Issues

Under Chapter VII, the Security Council formed three committees to address specific issues involving terrorism. The sanctions committee on Al-Qaeda and associated individuals and entities noted above is one such committee. A second such Security Council committee is the 1540 Committee, also discussed above. In addition, under Chapter VII and pursuant to Resolution 1373 (2001) the Security Council established the Counter-Terrorism Committee to monitor implementation of actions by States to combat terrorism.

Border Security Initiatives

Some UN resolutions urge countries individually to strengthen their overall border security efforts. For example, UNSCR 1325 on Women, Peace and Security has been interpreted as encouraging more female participation in conflict prevention and security, including border security. Additionally, the Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women (included in the UN Convention against Transnational Organized Crime) calls on States to enhance border controls to "prevent and detect trafficking in persons."[109] The Protocol also requests that States work to enhance coordination and communication among their respective border control agencies to effectively contribute to these goals.[110] UNSCR 2178 calls upon member states to strengthen national policies and coordinate information sharing to prevent foreign terrorist fighter from crossing their borders.[111]

Individual Country Sanctions and Controls

Generally, United Nations Member States adopt and abide by UN sanctions. In some cases, governments implement layered measures of control that go further and try to target changes in the sanctioned actors. As a European Commission document notes, "Sanctions are an instrument of a diplomatic or economic nature which seek to bring about a change in activities or policies such as violations of international law or human rights, or policies that do not respect the rule of law or democratic principles."[112]

In the recent case of Crimea, countries imposed targeted sanctions on Russia for its actions against Ukraine. Japan, the US and EU imposed their own sanctions independent of the UN.[113] Countries within the EU, including the United Kingdom, are obligated to comply with EU sanctions.[114]

Although countries may adopt comprehensive sanctions and export controls on paper, enforcement efforts may be more selective. One author claims that "no other international actor matches the USA's willingness to use sanctions…due to widespread reluctance towards sanctions in general and non-proliferation sanctions in particular."[115] Nonetheless some countries' export regulations are highly robust; Japan and Korea, for example, very tightly control retransfers of their technologies.[116]

OTHER INTERNATIONAL MEASURES

Many other international security initiatives affect trade and its facilitators, such as the finance and insurance industries. These include controls on the transport of hazardous materials, as seen in the Convention for the Physical Protection of Nuclear Material, as well as environmental sustainability measures required by the International Convention for the Prevention of Pollution from Ships (MARPOL).[117]

Regulations and oversight mechanisms often are spurred by emergencies. For example, prompted by the international financial crisis, G20 leaders established the Financial Stability Board in 2009 as "a mechanism for national authorities, standard setting bodies and international financial institutions to address vulnerabilities and to develop and implement strong regulatory, supervisory and other policies in the interest of financial stability."[118]

"Customs administrations have important powers that exist nowhere else in government… Customs can and should play a central role in strategic trade enforcement. Full implementation of the SAFE Framework will strengthen a Customs service's ability to detect, identify and interdict illicit shipments of proliferation concern; however, officers must be aware that proliferation trade is distinct from other forms of smuggling."

Simon Limage
Dep. Asst. Secretary for Nonproliferation Programs, US Department of State
Remarks at the WCO, Brussels, Belgium, November 15, 2012

To promote international standardization of customs processes, countries have set up Authorized Economic Operator (AEO) systems for companies that adopt customs security practices consistent with the World Customs Organization (WCO) SAFE Framework.[119] The SAFE Framework is a set of minimum standards that apply to Customs authorities and are integrated with AEO.[120] This involves standardization related to customs compliance, record-keeping, financial solvency, and security and safety.[121] In 2012, the WCO expanded the international capacity-building component, adding a section on coordination of border management and placing increased emphasis on mutual recognition processes.[122]

---

[80] See: World Customs Organization. "History." WCO in Brief. About Us. Accessed May 19, 2014. http://www.wcoomd.org/en/about-us/what-is-the-wco/au_history.aspx.

[81] United Nations Multilingual Terminology Database (UNTERM). "Zangger Committee Understandings." Accessed March 7, 2014. http://unterm.un.org/dgaacs/unterm.nsf/8fa942046ff7601c85256983007ca4d8/8e1ecde3952c7b1885256ffd004f2cd0?OpenDocument.

[82] Nuclear Suppliers Group. "History." Accessed July 24, 2014. http://www.nuclearsuppliersgroup.org/en/history1.

[83] The NSG includes all the countries involved with the Zangger Committee, plus Brazil, Cyprus, Estonia, Latvia, Lithuania, Malta, Mexico, New Zealand, Serbia, and South Korea.

[84] Nuclear Threat Initiative (NTI). "Nuclear Suppliers Group (NSG)." Treaties & Regimes. Accessed February 24, 2014. http://www.nti.org/treaties-and-regimes/nuclear-suppliers-group-nsg/.

[85] Good Practices for Corporate Standards to Support the Efforts of the International Community in the Non-Proliferation of Weapons of Mass Destruction. Vienna: Nuclear Suppliers Group. Accessed July 24, 2014. http://www.disseminate.eu/nsg/images/Files/National_Practices/NSG_Measures_for_industry_update_revised_v3.0.pdf.

[86] Strulak, Tadeusz. "The Nuclear Suppliers Group." *The Nonproliferation Review* (Fall 1993): 2-10. Accessed April 3, 2014. http://cns.miis.edu/npr/pdfs/strula11.pdf.

[87] The Australia Group. "Origins of the Australia Group." Accessed February 25, 2014. http://www.australiagroup.net/en/origins.html

[88] Bodell, Nenne. "International Security Cooperation Bodies." In *SIPRI Yearbook 2012: Armaments, Disarmament and International Security*, edited by D.A. Cruickshank, Jetta Gilligan Borg, David Prater, and Annika Salisbury, 505. Oxford: OUP, 2012.

[89] Arms Control Association. "The Australia Group at a Glance." Arms Control Association Fact Sheets. Last modified October 2012. Accessed February 25, 2014. http://www.armscontrol.org/factsheets/australiagroup.

[90] Ibid.

[91] Ibid.

[92] Nuclear Threat Initiative (NTI). "Wassenaar Arrangement." NTI Treaties & Regimes. Accessed February 21, 2014. http://www.nti.org/treaties-and-regimes/wassenaar-arrangement/.

[93] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. "Introduction." Accessed April 2, 2014. http://www.wassenaar.org/introduction/index.html.

[94] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. "How does the Wassenaar Arrangement work?" Accessed April 2, 2014. http://www.wassenaar.org/introduction/howitworks.html.

[95] *Guidelines & Procedures, including the Initial Elements*. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, July 2014. Accessed July 24, 2014.. http://www.wassenaar.org/guidelines/docs/5%20-%20Initial%20Elements.pdf.

[96] Boese, Wade. "The Wassenaar Arrangement." In *Challenging Conventional Wisdom: Debunking the Myths and Exposing Risks of Arms Export Reform,* edited by Tamar Gabelnick & Rachel Stohl, 173-181. Washington, DC: Federation of American Scientists, 2003.

[97] The Missile Technology Control Regime (MTCR). "Frequently Asked Questions." Accessed May 19, 2014. http://www.mtcr.info/english/FAQ-E.html.

[98] MTCR. "The Missile Technology Control Regime." Accessed April 3, 2014, http://www.mtcr.info/english/.

[99] MTCR, "Frequently Asked Questions."

[100] MTCR. "MTCR Guidelines and the Equipment, Software and Technology Annex." Last modified October 2013. Accessed April 2, 2014. http://www.mtcr.info/english/guidelines.html.

[101] MTCR. "Guidelines for Sensitive Missile-Relevant Transfers." Last modified October 2013. Accessed July 25, 2014. http://www.mtcr.info/english/guidetext.html.

[102] MTCR, "MTCR Guidelines and the Equipment, Software and Technology Annex."

[103] United Nations (UN). "United Nations Security Council Resolution 1540 (2004)." UN 1540 Committee. Accessed August 19, 2014. http://www.un.org/en/sc/1540/.

[104] Ibid.

[105] Crail, Peter. "Implementing UN Security Council Resolution 1540: A Risk-Based Approach." *Nonproliferation Review* 13, no. 2 (July 2006): 355-399. Accessed March 7, 2014. http://cns.miis.edu/npr/pdfs/132crail.pdf.

[106] United Nations Security Council. "UN Security Council Sanctions Committees: Security Council Sanctions Committees: An Overview." Accessed April 2, 2014. http://www.un.org/sc/committees/.

[107] Ibid.

[108] United Nations Security Council. "UN Security Council Sanctions Committees: Compendium of United Nations Security Council Sanctions Lists." Accessed April 2, 2014. http://www.un.org/sc/committees/list_compend.shtml.

[109] UN Convention against Transnational Organized Crime. *UNTS* 2225. November 15, 2000.

[110] Ibid.

[111] UN. "United Nations Security Council Resolution 2178 (2014)." Accessed October 20, 2014. http://www.un.org/ga/search/view_doc.asp?symbol=S/RES/2178(2014).

[112] *Sanctions or restrictive measures*. European Commission: European Union External Action, 2008. Accessed April 2, 2014. http://eeas.europa.eu/cfsp/sanctions/docs/index_en.pdf.

[113] Shankar, Sneha. "Japan Joins US, EU In Imposing Sanctions On Russia For Recognizing Crimea's Independence Following Referendum Termed Illegal By Western Nations." International Business Times, March 18, 2014. Accessed May 19, 2014. http://www.ibtimes.com/japan-joins-us-eu-imposing-sanctions-russia-recognizing-crimeas-independence-following-referendum.

[114] UK Department for Business, Innovation & Skills. "Sanctions, embargoes and restrictions." Guidance. Last modified July 17, 2014. Accessed July 25, 2014. https://www.gov.uk/sanctions-embargoes-and-restrictions.

[115] Brozska, M. "Role of Sanctions in Non-Proliferation." In *Arms Control in the 21st Century: Between Coercion and Cooperation*, edited by Oliver Meier and Christopher Daase, 142. London: Routledge, 2013.

[116] Glasgow, James, Elina Teplinsky, and Stephen Markus. "Nuclear Export Controls: A Comparative Analysis of National Regimes for the Control of Nuclear Materials, Components and Technology." Paper prepared by Pillsbury Winthrop Shaw Pittman, LLP for the Nuclear Energy Institute, Washington DC, October 2012. Accessed May 22, 2014. http://www.nei.org/corporatesite/media/filefolder/ExportControlsComparativeAnalysis.pdf.

[117] International Atomic Energy Agency. "Convention on the Physical Protection of Nuclear Material." International Conventions and Legal Agreements. IAEA Publications. Accessed May 19, 2014. http://www.iaea.org/Publications/Documents/Conventions/cppnm.html; International Maritime Organization. "International Convention for the Prevention of Pollution from Ships (MARPOL)." List of Conventions. About IMO. Accessed May 19, 2014. http://www.imo.org/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Prevention-of-Pollution-from-Ships-%28MARPOL%29.aspx.

[118] Financial Stability Board. "Our History." Accessed April 14, 2014. http://www.financialstabilityboard.org/about/history/.

[119] *Compendium of Authorized Economic Operator Programmes*. Brussels: World Customs Organization, 2014. Accessed May 19, 2014. http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/~/media/WCO/Public/Global/PDF/Topics/Facilitation/Instruments%20and%20Tools/Tools/Safe%20Package/AEO_Compendium.ashx.

[120] *SAFE Framework of Standards to Secure and Facilitate Global Trade.* Brussels: World Customs Organization, June 2012, 2. http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/~/media/55F00628A9F94827B58ECA90C0F84F7F.ashx.

[121] European Commission. "Authorised Economic Operator (AEO)." Customs Security. Policy Issues. Customs. Taxation and Customs Union. Accessed December 12, 2013. http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/aeo/.

[122] *SAFE Framework of Standards to Secure and Facilitate Global Trade*. Brussels: World Customs Organization, June 2012. Accessed April 28, 2014. http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/~/media/55F00628A9F94827B58ECA90C0F84F7F.ashx.

US Trade Controls

THE US EXPORT CONTROL SYSTEM

US export control measures reflect the objectives of key international regimes as well as US national security interests.

In addition to its membership in the major multilateral export control regimes, the US also participates in regimes established pursuant to the Nuclear Nonproliferation Treaty, the Chemical Weapons Convention, and the Biological Weapons Convention, as well as other conventions and informal agreements. The US also complies with UN resolutions on sanctions and export controls, such as UNSCR 1540, through an array of legislative, regulatory and enforcement actions. [123] However, it has not ratified some important international conventions and treaties, such as the Arms Trade Treaty.

In 2009, the Obama administration announced a sweeping overhaul of the US export control regime for the purpose of "strengthening national security and the competitiveness of key US manufacturing and technology sectors by focusing on current threats, as well as adapting to the changing economic and technological landscape."[124] Commonly referred to as export control reform (ECR), this interagency effort ultimately is intended to result in a single export control list, a single export licensing agency, a single lead export enforcement body, and a single information technology system.

While the administration has stated a goal of meeting these four ambitious objectives by 2016, there have been some remarkable interim steps to date. These include the transfer of licensing authority for many less-sensitive military technologies to Department of Commerce jurisdiction. ECR does not signal a change in US national security priorities or its international commitments, but rather is intended to better align US export control activities to address security concerns while also reducing the procedural burden on US exporters.

The project team, along with Stimson's Partners in Prevention Task Force, was concerned primarily with illicit trade in dual-use goods and technologies. This section therefore begins with a table capturing definitions of relevant terms from the Commerce Department's Export Administration Regulations. It then discusses the broader US export control regime as it exists today. It also discusses some of the changes brought about through ECR.[125]

Key Terms in Understanding US Exports of Dual-Use Goods and Technologies: Definitions from the Export Administration Regulations (15 CFR Part 772)

Deemed Export	The "release of technology or software subject to the EAR to a foreign national in the United States."*
End-User	"The person abroad that receives and ultimately uses the exported or reexported items. The end-user is not a forwarding agent or intermediary, but may be the purchaser or ultimate consignee."
Export	"An actual shipment or transmission of items out of the United States."
Exporter	"The person in the United States who has the authority of a principal party in interest to determine and control the sending of items out of the United States."
Forwarding Agent	"The person in the United States who is authorized by a principal party in interest to perform the services required to facilitate the export of the items from the United States. This may include air couriers or carriers."
Intermediate Consignee	"The person that acts as an agent for a principal party in interest for the purpose of effecting delivery of items to the ultimate consignee. The intermediate consignee may be a bank, forwarding agent, or other person who acts as an agent for a principal party in interest."
Principal Parties in Interest	"Those persons in a transaction that receive the primary benefit, monetary or otherwise, of the transaction. Generally, the principals in a transaction are the seller and the buyer. In most cases, the forwarding or other agent is not a principal party in interest."
Purchaser	"The person abroad who has entered into a transaction to purchase an item for delivery to the ultimate consignee. In most cases, the purchaser is not a bank, forwarding agent, or intermediary. The purchaser and ultimate consignee may be the same entity."
Reexport	"An actual shipment or transmission of items subject to the EAR from one foreign country to another foreign country."
Routed Export Transaction†	"A transaction where the foreign principal party in interest authorizes a U.S. forwarding or other agent to facilitate export of items from the United States."
Transfer	"A shipment, transmission, or release to any person of items subject to the EAR either within the United States or outside the United States."‡

* This definition is found at 15 CFR Part 734.2. All other definitions in this list are from 15 CFR Part 772.

† A Proposed Rule issued by the Commerce Department (70 Fed. Reg. 7,105 [Feb. 6, 2014]) would clarify the responsibilities of parties involved in export transactions where a foreign principal party in interest (PPI) is responsible for the export of items subject to the EAR, currently referred to as "Routed Export Transactions." The rule would institute a new term, "Foreign Principal Party Controlled Export Transaction", in the EAR to better define those instances where a foreign PPI responsible for the export of items subject to the EAR also assumes the authority and responsibility for licensing requirements.

‡ As explained at 15 CFR Part 734.2, *release* entails "visual inspection by foreign nationals of U.S.-origin equipment and facilities," "oral exchanges of information in the United States or abroad," and "[t]he application to situations abroad of personal knowledge or technical experience acquired in the United States."

AUTHORITIES

US exports are administered principally by the Departments of Commerce, State, Treasury, and Energy.[126] Other agencies, such as the Drug Enforcement Administration and the Food and Drug Administration, play lesser roles. Licensing advisory input is provided by certain elements of the Department of Defense and the Intelligence Community.

Responsibility for enforcement of export controls is also diffuse. Administrative enforcement is carried out by some of the aforementioned agencies, while criminal enforcement is the purview of the Departments of Justice, Commerce and Homeland Security.

As originally envisioned, ECR would consolidate licensing authority in a single agency, which would solicit recommendations from the interagency to ensure consistency.[127]

The current system derives principally from statutory mandates set forth in the Arms Export Control Act and the Export Administration Act.[128] The Arms Export Control Act (AECA), enacted in 1976, grants the president authority to control the import and export of all articles and services related to defense, a power formerly entrusted to the Secretary of State.[129] The AECA also establishes eligibility criteria under which states may receive defense services and articles, and how such articles and services may be utilized.[130] It requires that foreign governments only use these articles and services for approved purposes, such as self-defense. The provisions of the AECA are administered by the State Department's Directorate of Defense Trade Controls (DDTC).

The Export Administration Act (EAA) of 1979 allows the president to regulate US exports for reasons of national security, foreign policy, or short supply. It is the primary authority for dual-use export controls. Although the EAA expired in 2001 and has not since been reauthorized, the president has exercised the authority to enforce these controls under the authority of the International Emergency Economic Powers Act (IEEPA), which allows the president to implement trade controls after declaration of a national emergency.[131] The declaration issued in 2001 to invoke IEEPA was last extended in August 2014 for one year.[132] Associated administrative responsibilities are executed by the Commerce Department's Bureau of Industry and Security (BIS).

Oversight of US Exports: Relevant Agencies and Regulations

	Agency	Regulations	Purpose
	Department of State: Directorate of Defense Trade Controls (DDTC)	International Traffic in Arms Regulations (ITAR) 22 CFR Parts 120-130	Regulates the export of defense articles, services and technical data controlled under the United States Munitions List (USML)
	Department of Commerce: Bureau for Industry and Security (BIS)	Export Administration Regulations (EAR) 15 CFR Parts 700-799	Regulates the export of sensitive goods and technologies — including but not limited to so-called "dual use" items — controlled under the Commerce Control List (CCL)
	Department of Energy: National Nuclear Security Administration (NNSA)	10 CFR Part 810	Regulates activities of US persons engaged directly or indirectly in the production of special nuclear material outside the United States.
	Nuclear Regulatory Commission (NRC)	10 CFR Part 110	Regulates the import and export of nuclear material in and out of the United States
	Department of the Treasury: Office of Foreign Assets Control (OFAC)	Foreign Assets Control Regulations 31 CFR 500-599	Defines foreign and economic embargoes and sanctions that reflect United States foreign policy and national security interests
	Department of Commerce: Census Bureau	Foreign Trade Regulations (FTR) 15 CFR Part 30	Requires exporters to accurately file transaction and shipment information through the Automated Export System (AES)
	Department of Homeland Security: Customs and Border Protection (CBP)	Customs Regulations 19 CFR Parts 1-199	Defines the authorities and the regulations related to the transit of goods into and out of the United States

US companies exporting sensitive nuclear materials must receive authorization from the Secretary of Energy.[133] Companies must also receive authorization if engaging directly or indirectly in the production of special nuclear material within or on behalf of certain countries, like those that have not implemented full-scope IAEA safeguards.[134] The United States Nuclear Regulatory Commission identifies nuclear equipment, facilities and material subject to NRC licensing authority.[135]

CONTROL LISTS

There are two major lists of export-controlled items: the United States Munitions List (USML) and the Commerce Control List (CCL). Nuclear-related exports are subject to specialized controls administered by the Nuclear Regulatory Commission and the National Nuclear Security Administration in accordance with 10 CFR Parts 110 and 810, respectively.

The USML (22 CFR Part 121) is overseen by the Department of State, which has been authorized by the president under Executive Order 13637 to implement provisions of the Arms Export Control Act codified in the International Traffic in Arms Regulations (ITAR).[136] The USML regulates defense articles and services that are specifically designed for military application and that do not have a predominantly civilian application or an equivalent for use in civilian application. This list does not control or regulate items based on intention of use — all items are monitored under the presumption that they will be used for malicious purposes.[137]

The CCL (15 CFR Part 774) is overseen by the Department of Commerce, which has been authorized by the president to regulate the export of dual-use goods, software, and technology that originates in the US. The CCL is composed of ten categories that parallel those of the Wassenaar Arrangement: nuclear materials, facilities, and equipment; materials, organisms, microorganisms, and toxins; materials processing; electronics; computers; telecommunications and information security; lasers and sensors; navigation and avionics; marine; and aerospace and propulsion systems, including space vehicles.[138] The CCL is part of the Export Administration Regulations.

International trade in nuclear-related items and technologies is governed by the Nuclear Regulatory Commission and the National Nuclear Security Administration.[139] The NRC controls exports of nuclear-related items listed in 10 CFR Part 110. The NNSA grants special permission for US nationals to engage in the production of nuclear materials outside the US in accordance with 10 CFR Part 810.[140] While "outside the core" nuclear-related items are not subject to these regulations, they are not necessarily permitted for export, as some are controlled under the Commerce Department's Export Administration Regulations.

The Treasury Department's Office of Foreign Assets Control (OFAC) lists individuals and entities potentially involved in noncompliance with US trade embargoes and sanctions programs. Those on the Specially Designated Nationals and Blocked Persons List (SDNs) have their assets and financial activity restricted by the US government. In general, US nationals are prohibited from conducting business with these actors. SDNs may be affiliated with countries under US sanctions and embargoes, though some are members of non-state groups (such as terrorist groups and narcotics trafficking organizations).[141]

The Foreign Sanctions Evaders (FSE) list includes foreign actors that have either "violated, attempted to violate, conspired to violate, or caused a violation of US sanctions on Syria or Iran" or that have "facilitated deceptive transactions for or on behalf of persons subject to US sanctions." As with those actors directly targeted by US sanctions programs, US nationals and other actors residing within the US are prohibited from carrying out transactions with individuals and entities on the FSE list.[142]

US sanctions programs are guided in part by UN sanctions programs as well as other international mandates.[143] However, the US can and sometimes does pursue its own sanctions regimes in the absence of action by the international community. One example was seen in the July 2014 introduction of US sanctions following Russia's actions in Ukraine's Crimea region.[144] Even when based in part on UN sanctions, a US regime may impose further penalties and restrictions in accordance with its foreign policy and national security interests, as was seen in the case of Iran.[145]

In addition to items and specifically enumerated on control lists, the US operates "catch-all" controls similar to those employed by the Wassenaar Agreement, the Australia Group and the NSG. Catch-all controls prohibit exports when the exporter is in possession of knowledge that the end user intends to use the items in a WMD or missile program. An exporter must also forego a transaction if informed by the Commerce Department of an "unacceptable risk" an export will be used in a WMD program. Furthermore, the Export Administration Regulations (EAR) denote foreign "end-users" of concern to the US government. Exports to these entities require licensing, even for items not otherwise controlled.[146]

The US government presumes US companies understand potential applications of the items they export, particularly to ensure they cannot be used to impair national or international security. This presumption applies even when an export is completed entirely within the geographic United States, a transaction known as a "deemed export."[147] Transfers of controlled items or technical knowledge to a foreign national in the US are "deemed" to have been exported to that individual's country or countries of nationality.[148] Compliance with deemed export rules can cause significant challenges for foreign exchange students in STEM-related programs at US universities, to take just one example.

US Export Licensing Procedures

Export license applications are reviewed by a primary agency of jurisdiction, which assesses the level of risk associated with each transaction.

The Departments of State, Commerce, and the Nuclear Regulatory Commission evaluate license applications and render determinations considering the identity and affiliations of the applicant, the credibility and nature of the item's stated end-use, as well as any political, national security, or multilateral equities that may be affected.[149] While each responsible agency ultimately retains latitude in decision making, consensus and clearance among licensing and advisory agencies is the norm.

Under current export control procedures, US exporters must first determine the appropriate licensing agency for each product they plan to export. In most cases, this judgment can be made by the exporter based on past exports of similar items or clear design characteristics. When

jurisdiction remains unclear, exporters may file a Commodity Jurisdiction (CJ) request to obtain a definitive determination. Responsibility for rendering CJs rests with DDTC, though interagency consultation is integral to the process.[150]

In August 2009, President Obama created a task force to evaluate the need to restructure the US export control regime for sensitive items, including dual-use and nuclear materials. The task force included representatives from many stakeholder agencies, including the Departments of Defense, Transportation, and Justice, and the Office of the Director of National Intelligence. It concluded that the US export controls required major reforms in order to "better address current threats, and today's rapidly changing technological and economic landscapes."[151]

In April 2010, then-Defense Secretary Robert Gates delivered a landmark speech articulating the administration's view on what the priorities of a major reform effort should be. The US export control system, Gates said, needed a single licensing agency, a single control list, a single enforcement coordination agency, and an integrated IT system. [152] Several months later, the White House formally launched its ECR initiative to take these four overarching goals from concept to implementation.

With particular regard to a single export control list, the reform effort is following a so-called "bright line" approach in which officials first separate items that merit continued control on the USML from those that should be controlled on the CCL as dual use. Once that commodity-level review process has been completed, the administration plans to reconcile the USML and CCL in accordance with a three-tiered control framework. This challenging process, which is being advised by interagency experts led by DoD, is intended to produce a "positive" list based on objective design criteria.[153]

The table below offers a snapshot of the three broad implementation phases for ECR.

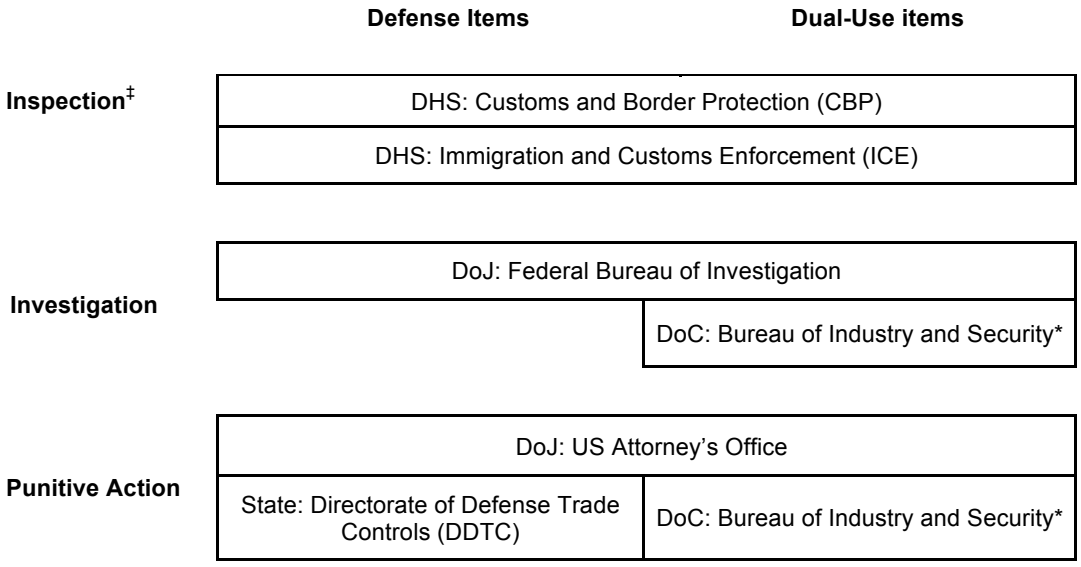
Objectives of the President's Export Control Reform Initiative

Phase	Control List	Licensing	Enforcement	Information Technology
I	Refine, understand, harmonize definitions to end jurisdictional confusion between two lists; establish new control criteria	Implement regulatory-based improvements to streamline licensing	Synchronize and de-conflict enforcement; create Enforcement Fusion Center	Determine enterprise-wide needs
II **(requires congressional notification and additional funding)**	Restructure two lists into identical tiered structures; apply criteria; remove unilateral controls where appropriate; submit proposals multilaterally to add/remove controls	Complete transition to mirrored control list; fully implement licensing harmonization	Expand outreach and compliance	Transition toward a single electronic licensing system
III **(requires legislation)**	Merge two lists into a single list; implement process for updating list	Implement single licensing agency	Consolidate enforcement activities under one agency	Implement a single system for licensing and enforcement

EXPORT ENFORCEMENT

As illustrated in the table below, numerous agencies are involved in the enforcement of US export controls for defense and dual-use items, be that in inspection at US ports, investigation of suspicious exports, or criminal or administrative punitive action against violators.[154] The export of sensitive of materials is not just limited to licensing and is a cross-agency effort to ensure US sensitive materials end up in the hands of the correct end-user.

Export Enforcement Agencies and their Primary Roles for Defense and Dual-Use Items[155]



‡ For purposes of this graphic, "Investigation" does not include pre- and post-shipment checks, such as those carried out through the Blue Lantern Program.

** Includes BIS Office of Export Enforcement*

Within each of these agencies are a variety of specialized offices and units supporting discrete aspects of export enforcement. For example, within DHS ICE, the Counter-Proliferation Investigations Unit prevents the export of sensitive materials, including WMDs, defense articles, dual-use items and small arms and light weapons.[156] The FBI has also instituted the Weapons of Mass Destruction Directorate that seeks to increase coordination between the Bureau's law enforcement, intelligence and technical departments to prevent the proliferation of WMD materials.[157] Another arm of ICE includes the Homeland Security Investigations (HSI) directorate, which conducts investigations against organizations that threaten US national security through illicit trafficking of people and products.[158]

The Director of the National Intelligence established the National Counterproliferation Center in 2005 to coordinate the counterproliferation efforts of the intelligence agencies, including the CIA, NSA and DIA.[159] The FBI also set up the Counterproliferation Center in 2011 to detect and deter the proliferation of all types of weapons, providing an overarching counterproliferation directorate for field agencies. At the Department of Defense, the Criminal Investigation Service (DCIS) within the Inspector General's office investigates the transfer of materials to prohibited nations and individuals.

The Export Enforcement Coordination Center (E2C2)

In November 2010, President Obama issued Executive Order 13558, establishing the Export Enforcement Coordination Center (E2C2). E2C2 was created "to coordinate and enhance criminal, administrative, and related export enforcement activities." This spans some 17 federal agencies, whose functional roles and missions range from licensing, to law enforcement, to end-use monitoring:

- Air Force Office of Special Investigations (DOD)
- Bureau of Alcohol, Tobacco, Firearms and Explosives (DOJ)
- Customs and Border Protection (DHS)
- Defense Criminal Investigative Service (DOD)
- Defense Intelligence Agency (DOD)
- Defense Security Service (DOD)
- Directorate of Defense Trade Controls (DOS)
- Federal Bureau of Investigations (DOJ)
- Immigration and Customs Enforcement, Homeland Security Investigations (DHS)
- National Nuclear Security Administration (DOE)
- National Security Division (DOJ)
- Naval Criminal Investigative Service (DOD)
- Office of Export Enforcement (Commerce)
- Office of Foreign Asset Control (Department of the Treasury)
- Office of the Inspector General (US Export-Import Bank)
- Office of the National Counterintelligence Executive (ODNI)
- US Postal Inspection Service (US Postal Service)

The director, a DHS officer, is assisted by deputy directors from the Departments of Commerce (Commerce) and Justice (DOJ), as well as an Intelligence Community liaison. Already, E2C2 has revealed inefficiencies within the US export control system: It found 60 percent of investigations were being pursued by two or more agencies without their knowledge. As E2C2 develops, the goal is to further improve the ability of agencies to pool their intelligence assets and expertise in the areas where they have experience and relevant authorities.

E2C2 receives no dedicated funding. In large part, this reflects a longstanding challenge of properly resourcing interagency mechanisms. Absent meaningful budgetary or personnel authorities, such mechanisms — even those backed by presidential directive in other respects — can falter. As noted above, E2C2 does receive in-kind resources embodied in Commerce and DOJ deputy directors and the Intelligence Community liaison. Beyond these three positions explicitly mandated by the November 2010 executive order, support for E2C2 depends on buy-in from participating agencies. Accordingly, agency personnel contributions to staff E2C2 have been limited and somewhat inconsistent. The Commerce Department, for instance, plans to assign just one analyst to supporting E2C2 on a full time basis during FY 2014 and 2015. Commerce has, however, requested dedicated funding of its E2C2-detailed deputy director, as well as two analyst positions in support of E2C2.

The penalties that accompany enforcement actions vary based on several factors, including: the specific law/regulation violated; whether the party willfully committed the violation, voluntarily disclosed it or had been previously alerted to it by authorities; and the enforcement authority's interpretation of relevant circumstances. A civil penalty can be assessed through an administrative action or a judicial suit. The government can pursue criminal penalties when there is some measure of intent by the violator. Even the submission of wrong information on an export declaration can lead to fines of up to $10,000 per incident and up to five years imprisonment.[160]

Penalties for Violations of US Trade Control Measures

Agency	Potential Criminal Penalties (per violation)	Potential Civil Penalties (per violation)
Commerce	EAA • Maximum Fine: $1 million • Maximum Imprisonment: 20 years* IEEPA (When EAA is in lapse) • Maximum Fine: $1 million • Maximum Imprisonment: 20 years*	EAA • Maximum Fine: $11,000 • Maximum Fine involving items controlled for national security reasons: $120,000* IEEPA (When EAA is in lapse) • Maximum Fine: $250,000 or "twice the amount of the transaction that is the basis of the violation"*
State	• Maximum Fine: $1 million • Maximum Imprisonment: 20 years*	• Maximum Fine: $1 million • Maximum Imprisonment: 20 years*
Treasury	• Maximum Fine: Up to $1 million • Maximum Imprisonment: Up to 20 years	• Maximum Fine: $250,000 • Possible suspension or debarment from government contracts • Possible forfeiture of property associated with violation

** All violators subject to denial of export privileges and suspension/debarment of government contracts*

PROGRAMS TO SECURE THE SUPPLY CHAIN

In January 2012, the Obama administration issued the National Strategy for Global Supply Chain Security to identify priorities for streamlining regulations and programs to combat threats to the supply chain.[161] The Strategy pays heed to both established and emerging threat areas, including cybersecurity.[162] It outlines a number of action items ranging from R&D planning to pilot programs that can assess relevant technologies, such as the hybrid shipping container and next-generation WMD detection mechanisms.[163] It also encourages legislative steps to formalize and increase cooperation with foreign governments.

A LONGSTANDING EMPHASIS ON IMPORTS

Globalization of production and trade networks has increased exposure of all countries, including the United States, to illicit actors and terrorists. While considerable attention has gone to import security regimes, adequate security at foreign ports provides the first layer of defense and is a crucial part of the security equation. Internationally, the shipping industry is guided by a variety of voluntary codes, including the International Maritime Organization's International Ship and Port Facility Security Code (ISPS code), which provides "a standardized consistent framework for evaluating risk, enabling Government to offset changes with changes in vulnerability for ships and port facilities through determination of appropriate security levels and corresponding security measures."[164] The ISPS code seeks to establish a framework to guide cooperation between government agencies, local security enforcement, administrators and the shipping industry.

C-TPAT: A Model for Public-Private Partnerships?

As the global flow of legitimate goods has grown, so has the transshipment of illicit items, including small arms, drugs, counterfeit products and dual-use materials. Because the government cannot realistically check every container, or even every risky container, they are increasingly relying on trusted trader programs with industry to both add eyes to the supply chain and improve overall compliance with the government's security standards. The focal point of this partnership is providing industry with benefits for voluntarily taking part in the program. One of the largest efforts has been the Customs Trade Partnership against Terrorism (C-TPAT), first introduced in November 2001 and codified under the SAFE Port Act of 2006. Companies opting to participate in C-TPAT must demonstrate adherence to specific security measures across their entire supply chains. Validated companies are entitled to certain trade benefits, including fewer cargo exams and expedited clearances. In turn, C-TPAT members agree to "best practices" that incorporates a security program that goes beyond the mandated C-TPAT guidelines — incorporated into the company's written policies. C-TPAT has become an industry standard and a pre-requisite for many importers when building their supply chain. This, ultimately, is the goal of the program in order to create business incentives for companies to abide by best-practices, and ensure their supply chain abides by C-TPAT's security standards.

Today, over 10,000 companies are part of C-TPAT, including carriers, logistics service providers, terminal operators and selected foreign manufacturers. However, third-party logistic service providers were not included in C-TPAT until 2008. While C-TPAT was focused solely on imports for its first 13 years, CBP and the Advisory Committee on Commercial Operations of Customs and Border Protection (COAC) have been developing an export-oriented component. CBP began accepting applications for the so-called "C-TPAT Exporter Entity" regime in September 2014.

Yet there remain concerns as to the adequacy of ISPS standards and the degree to which international ports are actually implementing them. In response, US government departments and agencies such as Customs and Border Protection (CBP), the US Coast Guard, the Transportation Security Administration (TSA), and the DoE have established programs to bolster the capacity of foreign ports to identify high-risk cargo. In 2002, CBP initiated the Container Security Initiative (CSI) to improve capabilities at key ports for target high-risk cargo before it reaches the United States.

However, many major trading partners are not part of CSI. In addition, as shipping routes face potential changes in the coming decade, there will be a need to adapt or expand CSI to better facilitate the addition of new hubs or transshipment points. While major ports in the Caribbean are part of CSI, only three ports in South America are part of the program (Santos, Brazil; Buenos Aires, Argentina; and Cartagena, Colombia)[165] and in Africa, only two (Alexandria, Egypt and Durban, South Africa).[166] The US government will need to build relationships with ports in these continents to ensure proper standardization, guarantee oversight of the customs and declaration process, and mitigate threats as traffic increases from new and emerging markets.

CSI is not the only initiative focused on foreign ports. The Coast Guard's International Port Security Program (IPSP) and the National Nuclear Security Administration's (DoE) Megaports Initiative both aim to build the capacity of seaports in developing economies, including those in Africa, the Caribbean and South America. These programs, however, only offer training and temporary service. Unlike CSI, they do not provide long-term oversight.

TSA has concentrated on improving security at foreign airports that serve US-bound flights. TSA conducts frequent risk assessments of these airports, and based on these assessments, the Capacity Development Branch provides technology, equipment and training to security-deficient airports, such as in Aruba, Bahamas, Bermuda, Haiti and Ireland.[167] This program has met with some problems, including proper maintenance and usage of security technology.[168] Nonetheless, it provides the US government with an idea of where the international air-cargo supply chain is weak and helps identify risky incoming cargo.

There also have been international efforts to improve port security, including the World Customs Organization's Container Control Program (CCP), launched in 2003. The CCP is a joint program with the United Nations Office on Drugs and Crime to "assist Governments to create sustainable enforcement structures in selected sea ports in order to minimize the risk of shipping containers being exploited for illicit drug trafficking, transnational organized crime and other forms of black market activity."[169] Its efforts are focused on training and capacity building for self-sustaining threat reduction.

The US continues to implement Customs Mutual Assistance Agreements with World Trade Organization members to improve knowledge on imports through information and intelligence exchanges that, according to CBP, "ultimately assist countries in the prevention and investigation of customs offenses."[170] These arrangements improve overall supply chain visibility for the United States, especially from countries that pose a heightened risk, such as China, Morocco and Nigeria.[171]

Although US government programs provide technology, training and oversight to foreign ports and agencies, surveillance of all cargo is impossible. As such, continued and expanded

partnerships with carriers, LSPs, and exporters and importers can fill gaps in the regimes of foreign or US government agencies. Moreover, where existing foreign and domestic oversight may be insufficient, such partnerships with legitimate supply chain firms can go far in addressing inadequacies in the current control network.

EXPORT VULNERABILITIES

US exporters do not currently face the same advance reporting requirements as importers.[172] The full implementation of ITDS should help speed processing times and make more information available in advance. But even with these changes, CBP and other agencies have limited resources to check exports for compliance with myriad trade controls. CBP traditionally has focused on "such export violations as smuggled currency, illegal narcotics, stolen vehicles or other contraband" but has further developed its targeting system over the years.[173] Even some within CBP, however, feel that the targeting regime for export transactions is highly immature.[174]

False declarations of commodities, end users, and end uses all pose risks. In 2013, a US citizen pled guilty for shipping over 6,000 pounds of carbon fiber to China via Belgium.[175] In another case, US officials discovered in 2006 that a company in Turkey had purchased US-origin specialized metals used for missiles and re-sold them to Iran.[176] The Turkish company supplied false declarations on end-user information and reported to the exporter that the materials "will not be exported from Turkey and will not be used for any nuclear, missile or chemical/biological weapons related applications."[177]

For government agencies with export monitoring mandates, identifying sound risk-informed criteria for post-delivery end-user checks is a major challenge. In analyzing defense articles and services, for example, a recent GAO report recommends export licensing agencies assess current end-user risk criteria and work with industry to make improvements. [178] The GAO also has raised concerns that export control reform may increase demands on Commerce Department compliance activities without a commensurate shift in government resources, increasing proliferation risk.[179]

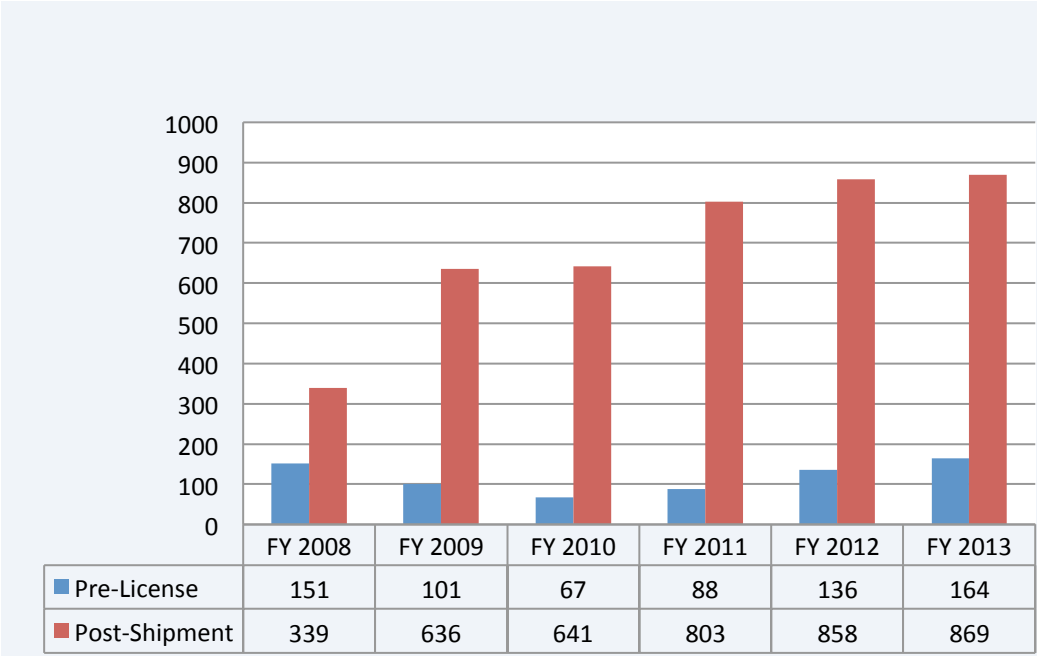
US Government End-Use Monitoring Programs

Program/Activity	Lead Agency	Items Monitored
Blue Lantern	Department of State	Defense Items on USML
Export Control Officers	Department of Commerce	Dual-Use Goods on CCL
Golden Sentry	Department of Defense	Government-to-Government Defense Goods
Sentinel Program	Department of Commerce	Dual-Use Goods on CCL

Notably, the Commerce Department's Bureau for Industry (BIS) employs seven Export Control Officers (ECOs) to help monitor exports of sensitive items to 29 countries, including China, Russia and the UAE. Like the State Department's Blue Lantern program, which regulates defense goods covered under the USML, ECOs conduct on-site end-user checks following the export of dual-use goods.[180] The ECOs' work is supplemented by the BIS Sentinel Program, which implements both end-use investigations and pre-shipment checks on buyers of sensitive dual-use items.[181] On the supply side, BIS's Project Guardian partners with manufacturers of dual-use items to flag suspicious requests.[182]

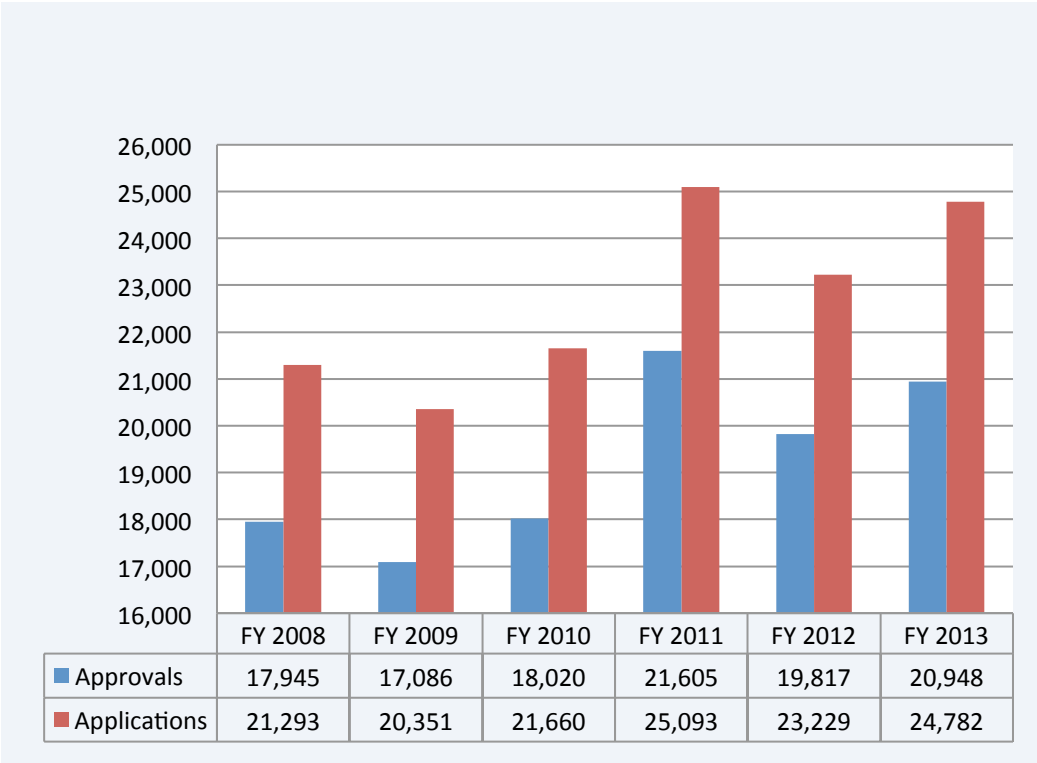
The two charts below provide an overview of the BIS licensing and verification activities.

BIS Pre-License Checks and Post-Shipment Verifications, FY 2008 – FY 2013[183]



	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
Pre-License	151	101	67	88	136	164
Post-Shipment	339	636	641	803	858	869

BIS License Applications Received and Approved, FY 2008 – FY 2013[184]



	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
Approvals	17,945	17,086	18,020	21,605	19,817	20,948
Applications	21,293	20,351	21,660	25,093	23,229	24,782

Department of Defense end-use monitoring programs include Golden Sentry, which monitors exports of US-origin defense articles and services that are sold or leased to foreign governments.[185] The goal of the program is to ensure that the registered end user is in possession of the article, a particular concern in areas of vulnerability for diversion or misuse such as in the Middle East. Managed by the Defense Security Cooperation Agency, Golden Sentry is maintained by the Combatant Commands, US Diplomatic Missions, the Defense Threat Reduction Agency and the Defense Institute of Security Assistance Management.[186]

While it may seem counterintuitive, another export-related threat centers on US domestic critical infrastructure. Namely, terrorist actors could plot to detonate an explosive in an outbound container, either at port or at another strategically chosen location along the domestic legs of its planned route. Fraudulent commodity declarations could allow dangerous materials to go unnoticed long enough for such an act.

Finally, a related but distinct challenge to security oversight – both in US territory and abroad – is rooted in the complexities of multi-modal freight transportation. Intermodal transfer points can be fraught with confusion over jurisdiction and responsibility, leading to breakdowns in information sharing that can be exploited for the introduction of contraband into the supply chain.[187] While a specific container may not be targeted for elevated risk, then, security gaps at various points in a multi-modal supply chain all increase the potential for illicit trafficking.

---

[123] DoS. *Additional information on measures taken to implement United Nations Security Council resolution 1540 (2004) by the United States of America*. October 2013. Accessed May 20, 2014. http://www.state.gov/documents/organization/216319.pdf.

[124] Export.gov. "About Export Control Reform." Accessed October 15, 2014. http://export.gov/%5C/ecr/eg_main_047329.asp

[125] "Other US Government Departments and Agencies with Export Control Responsibilities." Code of Federal Regulations, title 15, supplement no. 3 to part 730.

[126] Export.gov. "Export Licenses." Licenses and Regulations. Last modified April 27, 2011. Accessed May 21, 2014. http://export.gov/regulation/eg_main_018219.asp.

[127] LoC. CRS. *The US Export Control System and the President's Reform Initiative*. By Fergusson, Ian F., and Paul K. Kerr. January 13, 2014. Accessed February 28, 2014. http://www.fas.org/sgp/crs/natsec/R41916.pdf.

[128] Ibid.

[129] Ibid.

[130] The Arms Export Control Act (AECA). 22 US Code § 2778.

[131] Executive Order 13222. "Continuation of the National Emergency With Respect to Export Control Regulations." *Federal Register* 78, no. 155 (August 12, 2013): 49107.

[132] Executive Office of the President. "Notice to Congress — Continuation of the National Emergency with respect to Export Control Regulations." Accessed August 26, 2014. http://www.whitehouse.gov/the-press-office/2014/08/07/notice-congress-continuation-national-emergency-respect-export-control-r

[133] "Assistance to Foreign Atomic Energy Activities." Code of Federal Regulations, title 10, part 810.

[134] Ibid.

[135] "Licensing Requirements." Export and Import of Nuclear Equipment and Material. Code of Federal Regulations, title 10, part 110.5.

[136] "The International Traffic in Arms Regulations (ITAR)." Code of Federal Regulations, title 22, §120-130; DoS. "Overview of US Export Control System." Export Control and Related Border Security (EXBS) Program. Accessed April 4, 2014. http://www.state.gov/strategictrade/overview/.

[137] DoS, "Overview of US Export Control System."

[138] DOC. "Commerce Control List (CCL)." Bureau of Industry and Security. Accessed April 4, 2014. https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl.

[139] DoS, "Overview of US Export Control System."

[140] "Assistance to Foreign Atomic Energy Activities." Code of Federal Regulations, title 10, part 810

[141] US Department of the Treasury (US Treasury). "Specially Designated Nationals List (SDN)." Financial Sanctions. Resource Center. Last modified July 23, 2014. Accessed July 25, 2014. http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.

[142] Ibid.

[143] US Treasury. "Mission." Office of Foreign Assets Control (OFAC). Offices. Organizational Structure. About. Last modified July 23, 2014. Accessed July 25, 2014. http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx.

[144] US Treasury. "Ukraine-Related Sanctions." Programs. Financial Sanctions. Resource Center. Last modified July 23, 2014. Accessed July 25, 2014. http://www.treasury.gov/resource-center/sanctions/Programs/Pages/ukraine.aspx.

[145] BBC News. "Q&A: Iran sanctions." Last modified January 20, 2014. Accessed April 4, 2014. http://www.bbc.com/news/world-middle-east-15983302.

[146] DoS. "Overview of U.S. Export Control System." Accessed May 21, 2014. http://www.state.gov/strategictrade/overview/.

[147] DOC. BIS. "Deemed Exports." Policy Guidance. Accessed April 4, 2014. https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports.

[148] Ibid.

[150] DOC. BIS. "Commodity Jurisdiction." Licensing Guidance. Accessed August 22, 2014. http://www.bis.doc.gov/index.php/licensing/commerce-control-list-classification/commodity-jurisdiction

[151] McCormick, Beth. "Export Control Reform Update." Remarks made at the DOC, BIS Conference, Washington, DC, July 24, 2013.

[152] CRS, *The US Export Control System and the President's Reform Initiative*.

[153] Ibid.

[154] Government Accountability Office (GAO). *Export Controls: Challenges Exist in Enforcement of an Inherently Complex System*. December 2006, 8. Accessed April 3, 2014. http://www.gao.gov/assets/260/254812.pdf.

[155] GAO, *Export Controls*, 5-8.

[156] Immigration and Customs Enforcement (ICE). "Overview." Counter-Proliferation Investigations Unit. National Security. Accessed April 3, 2014. http://www.ice.gov/counter-proliferation-investigations/; Federal Bureau of Investigation (FBI). "FBI Counterproliferation Center." National Security Branch. About Us. Accessed April 3, 2014. http://www.fbi.gov/about-us/nsb/fbi-counterproliferation-center.

[157] Federal Bureau of Investigation (FBI). "Weapons of Mass Destruction Directorate." Just the Facts. Ten Years After: The FBI Since 9/11. About Us. Last modified September 2011. Accessed April 3, 2014. http://www.fbi.gov/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1/weapons-of-mass-destruction-directorate.

[158] US Department of Homeland Security (DHS). Immigration and Customs Enforcement (ICE). "Homeland Security Investigations." About ICE. Accessed April 3, 2014. http://www.ice.gov/about/offices/homeland-security-investigations/.

[159] Office of the Director of National Intelligence (ODNI). National Counterproliferation Center. "Home." Accessed April 3, 2014. http://www.counterwmd.gov/index.htm.

[160] Penalties for unlawful export information activities. 13 US Code § 305.

[161] White House. *National Strategy for Global Supply Chain Security*. Washington, DC: White House, January 23, 2012: 3. Accessed November 5, 2013. http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf.

[162] White House. *National Strategy for Global Supply Chain Security Implementation Update*. Washington, DC: White House, 2013: 3. http://www.whitehouse.gov/sites/default/files/docs/national_strategy_for_global_supply_chain_security_implementation_update_public_version_final2-26-131.pdf.

[163] Ibid., 11.

[164] International Maritime Organization (IMO). "ISPS Code." IMO Instruments. Maritime Security and Piracy. Our Work. Accessed December 4, 2013. http://www.imo.org/ourwork/security/instruments/pages/ispscode.aspx.

[165] DHS. CBP. "Container Security Initiative: Operational Ports." Last modified May 2011. Accessed December 19, 2013. http://www.cbp.gov/sites/default/files/documents/csi_brochure_2011_3.pdf.

[166] Ibid.

[167] GAO. *Aviation Security: TSA Has Taken Steps to Enhance Its Foreign Airport Assessments*, 26. http://www.gao.gov/new.items/d12163.pdf.

[168] Ibid., 25.

[169] United Nations Office on Drugs and Crime. "The UNODC-WCO Container Control Programme (CCP)." Accessed December 19, 2013. http://www.unodc.org/unodc/en/drug-trafficking/horizontal-initiatives.html.

[170] DHS. CBP. "Customs Mutual Assistance Agreements (CMAA) by Country." International Agreements. International Initiatives. Border Security. Accessed January 30, 2013. http://www.cbp.gov/xp/cgov/border_security/international_operations/international_agreements/cmaa.xml.

[171] Ibid.

[172] In the export process the carrier has to file a manifest with CBP four days after the departure; only freight forwarders who are approved by CBP have the option of submitting export data ten-days after departure. Non-approved freight forwarders must submit export data prior to export.

[173] DHS. CBP. *Privacy Impact Assessment for the Automated Targeting System*. By Landfried, Phil, and Hugo Teufel III. November 2006. Accessed June 2, 2014. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf; DHS. CBP. *Privacy Impact Assessment for the Automated Targeting System*. By Bush, Thomas, and Mary Ellen Callahan. June 2012. Accessed June 2, 2014. https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf.

[174] Author interviews with CBP officials.

[175] DoJ. *Summary of Major US Export Enforcement, Economic Espionage, Trade Secrets and Embargo-Related Criminal Cases*. March 2014: 11.

[176] Ibid., 45.

[177] Ibid., 46.

[178] GAO. *Implementation Gaps Limit the Effectiveness of End-Use Monitoring and Human Rights Vetting for US Military Equipment*. November 2011, 21.

[179] GAO. *US Agencies Need to Assess Control List Reform's Impact on Compliance Activities*. April 2012. Accessed May 13, 2014. http://www.gao.gov/products/GAO-12-613.

[180] Congress. House. Statement of Kevin J. Wolf before the Committee on Foreign Affairs. 113th Cong., 1st sess., April 24, 2013. Accessed January 30, 2014. http://docs.house.gov/meetings/FA/FA00/20130424/100744/HHRG-113-FA00-Wstate-WolfK-20130424.pdf.

[181] DOC. BIS. Office of Export Enforcement. "Compliance." Office of Export Enforcment (OEE). Enforcement. Accessed January 30, 2014. http://www.bis.doc.gov/index.php/enforcement/oee/compliance.

[182] DOC. BIS. *Annual Report to the Congress for Fiscal Year 2013*. Washington, DC: DOC, 2013: 16. http://www.bis.doc.gov/index.php/forms-documents/doc_view/866-bis-annual-report-to-congress-for-fiscal-year-2013.

[183] DOC. BIS. *Annual Report to the Congress for Fiscal Year 2013*; DOC. BIS. *Annual Report to the Congress for Fiscal Year 2012*. 2013. Accessed May 7, 2014. http://www.bis.doc.gov/index.php/forms-documents/doc_view/683-bis-annual-report-fy-2012; DOC. BIS. *Annual Report to the Congress for Fiscal Year 2011*. 2012. Accessed May 7, 2014. http://www.bis.doc.gov/index.php/forms-documents/doc_view/284-bis-annual-report-2011; DOC. BIS. *Annual Report to the Congress for Fiscal Year 2010*. 2011. Accessed May 7, 2014. https://www.bis.doc.gov/index.php/forms-documents/doc_view/656-bis-annual-report-2010; DOC. BIS. *Annual Report to the Congress for Fiscal Year 2009*. 2010. Accessed May 7, 2014. https://www.bis.doc.gov/index.php/forms-documents/doc_view/655-bis-annual-report-2009.

[184] Ibid.

[185] Defense Security Cooperation Agency (DSCA). "Golden Sentry." In Security Assistance Management Manual. April 2012. Accessed February 12, 2014. http://www.samm.dsca.mil/chapter/chapter-8#C8.2.

[186] Ibid.

[187] Pillai, Nishant. "Key Issues and Challenges in Intermodal Transportation Security." Presentation at the Transportation Research Forum, March 24, 2006. Accessed December 16, 2013. http://www.trforum.org/forum/downloads/2006_5CPillai_presentation.pdf.

Trade Stakeholders

OVERVIEW

What the policy community often reduces to the term "global supply chain" is actually a complex, multi-layered system of assets owned primarily by private sector entities. Industry and government alike leverage these assets in the air, sea, land, space and cyber domains, which collectively can be thought of as a public good that is shared across national borders. This physical and informational infrastructure has been critical to the rise of modern trade and production networks. But it also has substantial vulnerabilities.

The transportation of goods in and out of the United States involves a wide range of trade stakeholders. *Exporters* and *importers*, both international and domestic, depend on a web of actors to move their products from one point to another, using a variety of transportation modes.[188] Transportation of these products relies on *carriers*, who are responsible for ferrying the exporter's products through domestic and international jurisdictions.

The supply chain, however, is not simply importers, exporters and carriers, but is made up of a variety of additional actors that facilitate efficient, economic, safe and secure transport.

Logistics service providers (LSPs) function as centralized procurement organizers — aiding in the processing, warehousing, and movement of products along the international supply chain. The entire process may be overseen by one or more LSPs hired by the importer or exporter to coordinate the process. LSPs are instrumental in aiding small and medium-sized enterprises (SMEs) disentangle the complex US regulations, and ensure efficient delivery of their products. They are being increasingly utilized, evidenced by LSP revenues increasing 7-16 percent annually over the past five years.[189]

Wholesale traders are also being used with more frequency to export goods for SMEs. According to the United States International Trade Commission (USITC), wholesale trade includes transactions for "(a) goods for resale (i.e., goods sold to other wholesalers or retailers), (b) capital or durable non-consumer goods, and (c) raw and intermediate materials and supplies used in production."[190] Wholesale trading in exports has increased steadily over the past decade, providing industry, especially SMEs, with a channel to the global marketplace.[191]

Global trade volumes are increasing every year, as more and more freight forwarders, exporters, importers, wholesalers and carriers take advantage of business opportunities.[192] The US government's emphasis on increased exports, especially from SMEs, is only increasing the complexities in global value chains.[193] Pressure on SMEs to export will increase reliance on LSPs and wholesalers for risk mitigation.

Despite the expanding supply chain, risks remain — including as LSPs and wholesalers become bigger players in the process. The *ports* themselves, as well as *trade facilitators* such as the

insurance industry, play important roles helping industry address supply chain threats. Evaluating not only the security concerns but also each stakeholder's liability helps shed light on what security gaps remain and how they might be addressed.

EXPORTERS

US exports are on the rise. In 2013, total US exports of goods and services amounted to over $2.3 trillion. Exports have increased each year since 2009, owing among other things to the return of economic growth among trade partners — not least in the EU.[194] As to strategic goods, Commerce Department regulators in 2012 approved export licenses for items reflecting over $1.8 trillion in total value,[195][196] representing an increase of $300 billion over 2011.[197] The US also is a major arms exporter. In 2011, for instance, arms sales were estimated at $16.6 billion.[198]

It also is critically important to recognize the central role of services in contemporary cross-border transactions. According to USITC figures for 2011, research and development constituted 19 percent ($23.4 billion) of services exports. Installation, maintenance and repair of equipment represented another 11 percent ($13.8 billion).[199] Both of these sums marked significant annual increases.[200]

SMEs figure prominently in US exports. They supplied about 30 percent of merchandise exports over the 1997-2007 period and 35 percent of total exports in 2012.[201] In 2011, 98 percent of exporting firms were SMEs.[202] A corollary is that the activities of SMEs — along with wholesalers, as discussed above and seen again in the table below — merit special attention in the proliferation context.

Total Known Value of Exports from US SMEs and Wholesalers

	2008	2009	2010	2011	2012
Total for all Identified Enterprises	$1,147,669	$938,794	$1,137,635	$1,325,046	$1,379,683
SMEs*	$266,504	$283,562	$276,662	$316,174	$327,912
All Wholesalers	$248,195	$217,921	$268,334	$305,297	$307,135
Small and Medium Wholesalers	$124,538	$102,917	$126,822	$150,423	$151,841

** enterprises with fewer than 500 employees*

SECURITY AND LIABILITY

In general, exporters are responsible for safe packing, proper labeling and documentation, insurance requirements and regulatory compliance.[203] For the export of items controlled on the US Munitions List or Commerce Control List — administered respectively by the State Department and Commerce Department — exporters generally are required to obtain a license. Regardless of the type of item being transacted, exporters are liable for the conduct of various supply chain actors and the handling of both physical products and associated technical data.

To understand regulatory requirements for completing a given transaction, exporters must first determine whether the relevant items are subject to the EAR or ITAR.[204] When they are unsure, exporters may request a commodity jurisdiction determination from the Commerce Department's Bureau of Industry and Security or the State Department's Directorate of Defense Trade Controls.[205] In addition to EAR/ITAR requirements, exporters must determine whether a given transaction would violate OFAC sanctions.

Punishable violations of the ITAR, which regulates defense articles and services, are described in 22 CFR 127.[206] Punishable violations of the EAR, which regulates items with both military and civilian applications, are described in 15 CFR 764.[207] These two parts of the CFR also contain State Department and Commerce Department policy on companies' voluntary disclosures of potential violations.

The Treasury Department also regulates exports to prohibited persons and countries. Under the Treasury's Office of Foreign Assets Control (OFAC) laws and sanctions list, exporters are forbidden from exporting to countries, groups or individuals sanctioned under the Specially Designated Nationals (SDN) List, unless they obtain a license from OFAC.[208] When found to be in violation of these rules, transactions with sanctioned entities are subject to criminal penalties.[209]

Large firms typically have large compliance operations. Nonetheless, even these firms are sometimes penalized for violations. In 2012, HSBC was charged for laundering millions of dollars, including for two Mexican drug cartels. It ultimately settled with OFAC on terms that included a $375 million fine and forfeiture of another $1.3 billion for violations of the Bank Secrecy Act, the International Emergency Economic Powers Act and the Trading with the Enemy Act.[210]

In 2013, Raytheon agreed to pay $8 million in civil penalties for 125 charges of ITAR export violations.[211] Most of the charges were related to Raytheon's management of its Technical Assistance Manufacturing License Agreements,[212] including "inaccurate tracking, valuation and documentation of temporary exports and imports of controlled hardware, manufacture of such hardware by Raytheon's foreign partners in excess of the approved amounts, and failures to timely obtain and submit required documents."[213] Because Raytheon cooperated in the investigation and agreed to take certain remedial steps, US authorities did not pursue administrative debarment.[214]

In 2012, Pratt & Whitney Canada (P&WC) and ITS subsidiary companies, United Technologies and Hamilton Sundstrand, were charged with "the improper export to China of modifications to Hamilton Sundstrand engine control software incorporated into P&WC helicopter engines from 2002-2005."[215] Despite additional charges of false declarations and failure to inform the US

government in a timely manner on export of defense services, DOJ deferred action against United Technologies and Hamilton Sundstrand pending implementation of remedial steps, including strengthening compliance infrastructure.[216]

With large firms such as these having difficulty being fully compliant, smaller firms with less capacity and experience in exporting certainly face a challenge. These smaller firms constitute the vast majority of US businesses. In 2010, 99.7 percent of US enterprises were classified as small and medium enterprises.[217]

According to a 2010 USITC study, some of the main hurdles that deter SMEs from exporting manufactured goods include:

- Insufficient access to capital/financing for the underlying sale as well as unexpectedly high transaction costs (e.g., for transportation)
- Complex export regulations
- Small scale production which limits the ability to supply large-scale orders
- Tariff and nontariff barriers
- Lack of harmonization in foreign customs procedures and regulations
- Poor market intelligence for a given country/region[218]

While these obstacles might not be significant individually, they collectively make it difficult for these firms to enter into the export industry — creating confusion and uncertainty that deters their participation. A more recent USITC study on challenges SMEs face in exporting to the European Union noted their difficulty in demonstrating standards compliance or conformity assessment processes.[219] Better harmonization of standards and regulations internationally would help.[220]

Increasing exports became one of the major performance goals of the White House when it launched the National Export Initiative in 2010. Smaller firms have been expected to play a major role in this expansion.[221] To that end, several agencies — including the US Export-Import Bank, Small Business Administration (SBA), and various Commerce Department offices — have ramped up export promotion programs. For example, the US Export-Import Bank has emphasized its loans, loan guarantees and insurance coverage to exporting SMEs.[222]

Where SMEs do not have the in-house capabilities or capital to enter export markets, wholesalers often are willing to facilitate. These intermediaries are potentially worrisome from a security perspective — there are a variety of illicit schemes that have emerged from this practice, including reselling the product through opaque jurisdictions to nefarious end-users or selling the product at a higher profit and subsequently laundering the profits.

The Justice Department's *Summary of Major US Export Enforcement, Economic Espionage, Trade Secret And Embargo-Related Criminal Cases* shows multiple cases in which intermediary companies, both international and US-based, have purchased US goods and subsequently resold them to end users with nefarious intent. This is a particular concern for advanced technologies, which SMEs often export.[223] In 2008, Russian nationals exported microelectronics controlled under US export controls to Russia "frequently through

intermediary procurement firms, to Russian end users, including Russian military and intelligence agencies."[224] SMEs are willing to export through intermediaries but may not have the knowledge to identify illegal schemes or false declarations and invoices, putting these companies at risk of complicity in illicit trafficking.

Another worrisome phenomenon is known as trade-based money laundering. Intermediaries can buy goods (often with falsified documentation) and then re-sell at a higher price on the foreign market,[225] using opaque transaction reporting laws in countries such as Switzerland to obscure profit margins.[226] The revenue is then channeled to offshore companies and banks.[227] Not only does this practice deprive the original producer of profit, but the associated tax evasion also curbs government revenue.

A further challenge is the transfer of trade secrets and information on export controlled goods, or "deemed exports." According to BIS, deemed exports include "any release of technology or source code subject to the EAR to a foreign national…such release is deemed to be an export to the home country or countries of the foreign national."[228] Companies and other organizations involved in research and development, such as universities, are particularly at risk for improper documentation on export controlled items.[229]

There is particular concern with foreign nationals working for US companies accessing technology or source data that is protected under export controls. The Justice Department has documented numerous cases of illegal technology and data transfers resulting in the stealing of trade secrets. For example, in 2012 a Chinese national was convicted of transferring military technical data on rockets and unmanned aerial vehicles to Chinese government officials and presenting the information at several conferences at Chinese Universities.[230] According to DOJ reports, the Chinese national's US employer had trained the employee in export control laws.

Despite such cases, the full breadth of risks in transferring technology or source data is only slowly coming into view. The project team found this to be an area that industry has not yet earnestly focused on but that likely will be a particular concern in future non-proliferation efforts. While industry is indeed becoming more alert to the theft of trade secrets, many SMEs and research institutions do not seem to appreciate the nuances of what information is controlled and what protocols must be followed in transferring controlled information.

LOGISTICS SERVICE PROVIDERS

A logistics service provider (LSP) acts as a centralized procurement actor, organizing the flow of commodities and cross-modal transactions along the supply chain — aiding in the processing, warehousing, and movement of products among and within countries. LSPs play a key role in facilitating transactions and the movement of goods, and their stake in the supply chain is only growing. From 2010 to 2011, the global 3PL industry's revenue grew from $541.6 billion to $616.1 billion.[231]

Third party logistics firms (3PLs) represent the largest category of logistics service providers,[232] and "typically specialize in integrated warehousing and transportation services that can be scaled and customized to customer's needs based on market conditions and the demands and delivery service requirements for their products and materials."[233] Under this umbrella are

included freight forwarders, brokers, consolidators and non-vessel operating common carriers (NVOCCs). 3PLs can provide some or all of the following services:

- International and domestic road, air and ocean transportation
- Warehousing
- Shipment consolidation
- Customs clearance and brokerage
- Cross-docking services, e.g., transferring cargo from railcar to containership
- Value added services, e.g., packaging and labeling.
- Order entry, processing and fulfillment
- Supply chain planning services[234]

3PLs can be broken down into three types of service providers: *basic*, *value-added*, and *logistics integration*:[235]

- Basic service providers provide warehousing services, arrange for processing and help select transportation carriers. These include non-asset-based 3PLs "who perform duties such as quoting, booking, routing, and auditing" transportation services; they lack their own vessels or warehouses.[236]

- Value-added service providers, in addition to the responsibilities of the basic service providers, arrange customs, logistics information systems and transportation fleet management. Freight forwarders fall within this category — providing services that focus on cost and logistics of transportation. Freight forwarders arrange 90 percent of heavyweight international air shipment, and 75 percent of less-than-container load revenues in maritime shipping.[237]

- Direct carriers — companies that have direct operational control of transport mechanisms — rely on freight forwarders and value-added service providers to market their services to exporters/importers.

Finally, logistics integrators take full responsibility for key supply chain operations from start to finish, and are critical in shaping the supply chain for individual products. Logistics integrators are embedded within the supply chain and create an agile omni-channel network.[238] NVOCCs can be considered logistics integrators; while they do not actually own their own vessels, they may own or lease containers and issue their own bills of lading and are responsible for the shipment.[239]

LSPs have been increasingly used since the 2008 economic crisis, when commercial pressures led companies to look for more cost-effective performance. LSPs have developed new ways to improve logistics and overall supply chain agility and flexibility — reducing shipping prices and increasing efficiency.[240] In 2014, shippers were able to cut logistics costs by 11 percent

year-over-year by using LSPs.[241] LSPs do this by integrating big data on the supply chain to identify optimal macro- and product-specific patterns for routing shipments.[242]

Many companies, especially smaller companies, cannot afford maintaining up-to-date supply chain knowledge and expertise. By using LSPs, producers can cut overhead by not relying on in-house, prohibitively expensive experts.[243] For example, when importing into the United States, LSPs obtain a certified customs broker license to have goods clear customs. The license involves a rigorous exam process, which gives the broker the authority to assist importers with Federal requirements for obtaining clearance. For small shippers and companies, maintaining their own in-house certified customs broker is often too expensive.

Furthermore, LSPs can afford to lower costs for companies, since collaborative distribution across the supply chain provide the LSPs with the ability to negotiate better rates amongst carriers, warehouses and consolidators.[244] However, the power of LSPs is based on long-term, mature contract relationships between the exporter and LSPs, providing specialized knowledge of the company's supply chain and needs.[245] While companies may be tempted to approach different LSPs, the 2014 Third-Party Logistics Study reports that successful shipper-LSP relationships are based on trust and specialized knowledge.[246]

Given how much smaller exporters typically rely on LSPs, including freight forwarders, for guidance, Stimson found in discussions with industry that forwarders were often frustrated by the amount of time they spent educating smaller and/or infrequent exporters on compliance and due diligence requirements. The forwarders manage huge flows of documents every day and having a blank or wrongly-coded entry takes up their precious time. Exporters in turn become frustrated at all the LSPs questions and information requirements for correctly and completely filling out export forms. The exporter may then turn to a LSP who has more lax standards and less questioning on the accuracy of the information being put in the forms.

To reduce the time that logistics service providers have to spend educating their clients and to demonstrate that they are not being capricious in their requests for information, the National Customs Brokers & Forwarders Association of America (NCBFAA) developed a best practices guide so that the forwarders could educate the parties doing the exporting. This best practices document is for exporters — not the logistics providers — and is continually updated.[247]

LSPs are playing an increasing role in supply chain security — leveraging their unique position across the supply chain to provide flexible measures to prevent thefts, tampering, smuggling and terrorist attacks. There are a variety of ways LSPs can maintain supply chain security, including:

- Ensuring physical security for goods
- Developing and instituting security procedures with their customers and contractors in the supply chain
- Providing alerts when shipments deviate from the planned supply route due to threat or weather
- Scanning shipments at key and potential weak points
- Obtaining security related certifications, such as C-TPAT

- Providing alternative routing for shipments in the event of supply chain disruption[248]

Successful supply chain security is based on two over-riding principles leveraged by LSPs: minimizing the number of touches in the supply chain and ensuring supply chain visibility.[249] One logistics provider can control and minimize the number of touches cargo is subject to along the supply chain, lowering the number of times that cargo passes through an intermodal or transshipment point. LSPs are also modernizing their IT capabilities to increase visibility along the entire supply chain. With one LSP tracking a shipment along the entire supply chain, discrepancies and differences in information can be mitigated.[250]

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

More and more LSPs are becoming C-TPAT certified. C-TPAT certification ensures that members follow a set of supply chain security standards to mitigate terrorist threats. As of December 2013, 944 logistics service providers and consolidators, as well as 856 brokers were C-TPAT certified.[251] This is an increase from 2011, when there were only 32 C-TPAT certified 3PLs. For a LSP to become C-TPAT certified it must be involved in the handling and/or management of cargo in the international supply chain, be licensed or bonded by the Federal Maritime Commission, Transportation Security Administration, CBP, or Department of Transportation, must maintain an office in the United States, and must meet certain security standards. While legislation has been proposed to allow non-asset based 3PLs to become eligible for C-TPAT certification, as of May 2013,

Non asset-based 3PL's who perform duties such as quoting, booking, routing, and auditing (these type of 3PL may possess only desks, computers, and freight industry expertise) but do not own warehousing facilities, vehicles, aircraft, or any other transportation assets, are excluded from C-TPAT enrollment as they are unable to enhance supply chain security throughout the international supply chain.[252]

C-TPAT security standards for LSPs include ensuring secure business partnerships "consistent with the C-TPAT security guidelines to enhance the integrity of the shipment at point of origin"[253] — screening customers along the supply chain and ensuring that all contracted service providers commit to C-TPAT guidelines.[254] Certified LSPs are expected to ensure that all contracted service providers maintain adequate security standards, including proper containers, container seals and container storage (including physical security at warehouses), as well as adequate conveyance inspection procedures.[255] It is expected that LSPs "must have procedures

in place to maintain the integrity of their trailers at all times"[256] — implementing proper conveyance tracking technology. In turn, C-TPAT members are rewarded with benefits, including access to fast-lanes and fewer inspections.

While C-TPAT membership continues to grow, there is a divergence in opinion within industry on the effectiveness of the program, and whether the benefits outweigh the cost of compliance. In a recent survey completed by the Advisory Committee on the Commercial Operations of Customs and Border Protection (COAC), logistics service provider respondents[257] were split 50-50 on whether C-TPAT was of value for their customers.[258] However, the industry has noted that as supplier contracts with major companies are requiring C-TPAT certification as a condition of a bid, these suppliers will likewise look to C-TPAT certifications from their logistics service providers.

LSP LIABILITIES

The liabilities on logistics service providers (LSPs) are complex and depend on the specific contractual terms they enter into with exporters/importers. Generally, LSPs are liable for damage or loss of goods during carriage and the costs of delay in the delivery due to the LSP's error if it is the principal contractor[259] or owner of the bill of lading.[260] Again, whether the LSP is the principal contractor or the owner of the bill of lading depends on the contract. In general, LSPs are not liable for cargo damage or loss — however if they designate themselves as the carrier, such as surface freight forwarders or indirect air carriers, they take on the reasonability of carrier liability.[261]

That being said, if the LSP is not the designated agent, it "is usually the shipper/owner, rather than the freight forwarder, who actually enters into the transportation contracts with the carriers" and thus the LSP is not liable for loss or damage.[262] However, the freight forwarder as an agent is liable if the plaintiff "can show (1) the carrier caused injury to the plaintiff's property or person through negligence, recklessness or intentional misconduct and (2) the shipper did not exercise reasonable care or perform proper due diligence when it screened, vetted, and selected the carrier to move the shipper's freight."[263]

Routed Export Transactions: Trust but Verify

In the normal export process, the United States Principal Party in Interest (USPPI) is responsible for filing the proper information through the Automated Export System (AES), including ensuring that all information is true, accurate and complete. However routed export transactions are an exception in terms of liability. A routed exporter transaction is when a USPPI allows the Foreign Principal Party in Interest (FPPI) to authorize a US freight forwarder, LSP or agent to move a shipment overseas. If the FPPI designates a US agent to carry out the shipment, the agent must obtain a power of attorney or written authorization from the USPPI or FPPI to file documentation for export, stipulated in the contract.

Under Part 748 of the Export Administration Regulations, the USPPI assumes all responsibility and liability for licensing, unless the FPPI is granted authority in writing, which makes the FPPI's authorized US agent the exporter. Thus, the agent of the FPPI takes on the responsibilities and liability of export and licensing. That being said, in a routed export transaction, "all parties to the transaction are subject to the fines and penalties when there is a violation."

Since the USPPI is putting an export under the control of an agent of the FPPI, and thus losing control of the shipment, there is a certain amount of trust the USPPI must place in the two other parties. Already there is an embedded risk with shipping hazardous materials (HAZMAT) and dual-use goods, and in the case of the former, US companies have guidelines on proper shipping. The USPPI must ensure that the contract with the FPPI's agent delineates clear security plans in order to avoid being penalized for inadequate security and risk measures if the cargo goes missing or results in damages. Furthermore, a routed export transaction does not remove responsibility from the USPPI to ensure proper verification of end users.

To remedy confusion stemming from Census's distinct definition of "routed export transactions" in the Foreign Trade Regulations (FTR), in February 2014, the Department of Commerce's Bureau of Industry and Security issued a Proposed Rule that would add the term "Foreign Principal Party Controlled Export Transaction" to describe the transactions currently permitted under the Export Administration Regulations (EAR) § 758.3(b) and described as "routed export transactions."

As an agent, an LSP can also be liable for errors and omissions, such as releasing cargo without a proper bill of lading or wrongly transcribing a code in a document. When exporters leave blanks in their export documents, they will often ask freight forwarders for help in completing the forms. The Stimson Center was told that responsible freight forwarders then direct exporters to complete key parts of the form by using the previously mentioned NCBFAA-prepared guidance. However, to the extent LSPs provide advisory services, they have some liability for the accuracy of that advice. They are also responsible for ensuring that they themselves do not knowingly facilitate violations of law or regulations.

From 2002-2006, BIS found that DHL had unlawfully aided and abbeted the shipment of unlicensed US export to Iran, Syria and Sudan. According to BIS reports, DHL had failed to comply with recordkeeping requirements for licensed goods.[264] DHL ultimately paid a $9,444,744 civil penalty and agreed to carry out external audits on exports to Syria, Iran and Sudan. As one law firm noted, "These charges are consistent with the BIS trend of increasingly focusing on 'causing' and 'aiding and abetting' scenarios in addition to seeking to enforce directly against the exporter."[265] More recently, Houston based Weatherford International Ltd paid $50 million in civil penalties imposed by BIS and OFAC and $50 million in criminal fines to DoJ for illegally exporting oil and gas equipment to Iran, Cuba and Syria — the largest BIS levied civil penalty.[266] BIS also alleges that Weatherford illegally transferred items protected by nuclear non-proliferation export controls.

As facilitators of trade, LSPs are approached to expedite many types of transactions. When presented with a suspicious or likely illicit transaction, they can choose to do the transaction, to ask for clarification — such as licensing requirements regarding appropriate product coding or the end user, or they can reject the shipment request. When the shipments are rejected, the LSPs can choose to report the request as suspicious or not. In discussions with industry, Stimson found that even larger facilitators would debate how to handle requests that were apparently illegal.[267]

CARRIERS

The four main "modes" of transport are air, rail, motor and ocean.[268] For a given shipment, the mode(s) used depends on a variety of factors, including product type, ultimate destination and the transport provider guidelines.

Around 90 percent of the world's commerce by volume is transported via maritime shipping, following the highly trafficked ocean routes that circumvent the entire globe — connecting major ports across Europe, North America, Asia and the Middle East.[269] Motor and rail carriers, on the other hand, are the main players for intra-North American trade. In 2012, rail and motor carriers accounted for nearly 75 percent of total trade by volume (not including oil) with Canada, and over 50 percent of trade with Mexico.[270] Rail trade itself with Mexico has quadrupled over the past ten years.[271] While air carriers convey less than one percent of the total US merchandise trade by volume, they provide faster delivery times — and for certain products, efficiency is a necessity.[272]

CARRIER LIABILITIES

All carriers, of course, have to comply with laws and regulations governing exports and sanction regimes. For example, US carriers are restricted from providing transport services to Cuba.[273] Carriers must also comply with other international regimes and treaties the United States has signed, such as the requirement for maritime vessels to take certain actions to decrease the likelihood of environmental damage from ships and to address any resulting environmental liabilities.[274]

To assess liability amongst carriers, it is necessary to distinguish transport modes — rail, motor, ocean and air. In general, carriers are liable for their shipments unless they can prove that the damage or loss was not caused by their own negligence.

Motor carriers under receipts and bills of lading are liable for damage, destruction and loss of cargo under 49 US Code 14706.[275] A rail carrier's liability is covered under 49 US Code 11706, which stipulates that the rail carrier is liable to whomever is owed the actual losses from the damaged or lost property.[276] In both rail and motor carrier cases, the liability encapsulates damage done by the receiving and delivering carrier, as well as "another carrier over whose line or route the property is transported in the United States or from a place in the United States to a place in an adjacent foreign country when transported under a through bill of lading."[277]

Liability for ocean carriers is primarily covered under two acts which define and limit liability: the Harter Act and the Carriage of Goods by Sea Act (COGSA).[278] The Harter Act, unless noted

in the domestic carriage's bill of lading, covers domestic transportation and in the time before lading.[279] Under the Harter Act, the carrier is not exempted from cargo loss unless adequate due diligence is exercised before the journey.[280] COGSA covers transportation between US ports and foreign states, and maintains that the carrier is liable for loss or damage arising from negligence to exercise due diligence and provide a seaworthy vessel, and the carrier must account for proper handling of cargo while onboard.[281] That said, carriers can file for 17 different defenses if claims are brought against them.[282]

Air carriers are governed separately for domestic and international commerce. For domestic, in general the air carrier is liable for loss, damage or threat as a result of negligence on behalf of the carrier.[283] The terms of liability are often stipulated in the bill of lading. Internationally, air carriers are governed by the Warsaw Convention which stipulates that the air carrier is liable for damages or loss due to negligence[284] and the burden of proof is on the carrier to show that the damage was not a result of negligence.[285]

In 2010, Maersk Lines Limited settled for $3 million dollars for OFAC allegations that Maersk had violated sanctions. OFAC claimed that Maersk had over 4000 shipments in and out of Iran and Sudan from 2003 to 2007.[286] Maersk, however, provided OFAC with large amount of information regarding the transfers, which resulted in a lower settlement.

There has been discussion of the reach of US law to foreign entities and companies. All entities organized under US laws, foreign entities owned by US entities, and anyone in possession of US goods is subject to US sanctions and export laws.[287] While there remain questions regarding the jurisdiction of US sanctions, most foreign entities will tend to avoid either doing business with US sanctioned countries or fighting OFAC allegations in order to avoid being deemed a 'specially designated national' — a business death sentence for foreign companies.[288]

PORTS

The United States has three main types of ports, generally distinguished by ownership: public seaport terminals, privately owned ports that provide services to shipping public, and ports that have no public access (for example industrial ports connected to a particular industry.)[289] However, in the United States, public ports are not governed by a national entity. While the waterways are managed by the United Coast Guard, public ports (the former two distinctions) are governed by either administrative divisions of the local or state government or by a port authority that is set up by state legislation.[290] Port authorities have a variety of purposes, but "all share the common purpose of serving the public interest of a state, region or locality."[291]

Foreign Trade Zones and Supply Chain Security

The use of Foreign Trade Zones (FTZs) has exploded since the 1990s. However, the increased use of FTZs has sparked security and trafficking concerns. Companies that are part of FTZs are vetted by CBP, including background checks on employees, an assessment of facility security, and ensuring the integrity of the inventory control and data systems. CBP also requires all companies to log how they handle merchandise at all points while in the FTZ. The Congressional Research Service concludes that because products often stay in the FTZ for longer than normal imports, the merchandise is often subject to longer exposure to audits and inspection. Despite this, the Financial Action Task Force notes that the repackaging and relabeling process can be difficult to monitor. Diversion is possible, especially for merchandise in in-bond trading and transshipment, which is subject to less vigorous oversight by CBP.

FTZs were created in 1934 from the Foreign-Trade Zones Act, to increase US trade as a result of increased tariffs during the Great Depression. FTZs are restricted areas, usually close to major ports, which are not within the customs authority of the United States. These zones are home to manufacturing and industry which manufacture the raw goods into finished products to be "exported" into the US commercial market. FTZs are usually utilized as a way of combining foreign inputs with domestic inputs. For example, crude oil, which made up 72 percent of FTZ input shares in 2012, is processed into by-products including gasoline, kerosene, jet-fuel, and petrochemicals. The total value of exports from FTZs into the US market increased from about $100 billion in 1993, to nearly $700 billion in 2011, making up 15 percent of the total US goods imported into the United States. Because of the increased use and economic advantages of FTZs for the US economy, CBP has increased the use of ACE within FTZs – increasing processing times. Because FTZs have unique reporting requirements, government agencies and private industry have cited the fact that not all these processes have been incorporated into ACE.

Imports into FTZs are not charged tariffs until they leave the FTZ and enter US commerce. The lack of tariffs saves US companies money and helps employ local populations to develop products. With crude oil, for example, the tariff for importing crude oil directly into United States is more expensive than the tariff for import of petrochemicals. Thus, a company producing petrochemicals can refine crude oil in the FTZ and pay a lower tariff for import of the final product — insourcing production in the US, employing locals, and making US companies more competitive in export-markets.

Despite not initially going through the normal CBP process for imports, CBP still ensures oversight of shipments entering the FTZ. Goods are still reported as a general import. Zone operators must file a request for permission to move goods into an FTZ, and imports from abroad are provided a permit for admission once CBP has determined the goods do not require a physical examination. According to CRS, in most cases, low risk cargo enters FTZs without examination.

LIABILITIES

Under the aforementioned COGSA, port terminal operators (Operator) "shall not be liable for any loss/damage to or in connection with the goods in an amount exceeding $500 US per package."[292] Operators are liable for damage or loss of goods if there is proven Operator negligence.[293] For example, in general, if there is an act of terrorism that damages or destroys a customer's goods, the operator is not liable for the damages unless they arose from the fault or negligence of the operator.[294]

The customer assumes responsibility for its vessels while in the port, and the operator is not responsible for inspection or monitoring the vessel. The customer assumes all responsibility "for watching, securing, and protecting the vessel, and all liability for any loss/damage to the

vessel shall rest solely with customers, except to the extent such loss/damage is caused both solely and directly by the negligence of Operator."[295] In turn, the customers are responsible for carrying out inspections before they begin using the port or leased equipment. This includes storage and warehousing — where the port operator "shall be responsible for exercising reasonable care under the circumstances… and shall not be liable for any loss, damage or injury to the goods that could not be avoided by exercise of such reasonable care."[296]

Although ports may be liable for security, they do not appear to have a role in export/sanctions enforcement.

INSURERS

Exporters, logistics service providers, carriers and ports all manage their risks, including their liabilities, by engaging with the insurance industry. Providers within the industry focus on specialties such as: logistics service providers, carriers such as marine or air, marine terminals and port authorities. Insurance may be provided for property and casualty losses, including business continuity coverage and third-party losses. Insurers cannot pay fines or penalties directly but can cover the cost of litigating against claims or defending against regulatory actions.

The insurance industry not only provides coverage to those involved in trade but also is liable for its own compliance with US laws and regulations. OFAC sanctions have been of particular concern to the industry and to reinsurers in particular as they typically do not know the client policies directly. Possible infractions include a policy holder becoming an SDN, beneficiaries of a policy being resident in a sanctioned country, or an employee of a foreign company with a global health insurance policy being a national of a sanctioned country.

There are numerous examples of insurance companies violating OFAC sanction regimes. For example, in 2011, General Reinsurance Corporation remitted $59,130 in order to settle a claim that the General Reinsurance had issued to reinsurance claims for Steamship Mutual Underwriting Association Limited for losses arising from an Iranian owned shipping company — a violation of the Iranian Transactions Regulations.[297] In another violation of the Iranian Transactions Regulations, HCC Insurance Holdings, Inc. paid $38,448 to settle allegations that HCC had participated in an insurance policy that insured a foreign-based commercial airline company that operated in Iran. For customer transactions, the industry will often include language in their policies that explicitly excludes coverage that would violate US sanctions.[298]

COMPLIANCE CHALLENGES

Relationships among private industry players are fairly well defined. The liability regimes and contracts outline the responsibilities in commercial transactions, although lawsuits still result over differences in interpretations. The International Chamber of Commerce helps to facilitate international trade understanding by providing standard contract terminology known as Incoterms [add Trademark designation].[299] A problem arises, however, in the challenging relationship between the private sector and government, with the latter having power to fine, prosecute, and otherwise challenge industry on its compliance with laws and regulations.

Fines for non-compliance do not appear large given the size of many of the companies. If JPMorgan can absorb $13 billion in a settlement with the Justice Department over mortgage quality,[300] then the money laundering and sanctions violations fines ranging from $32,400 to $1.92 billion on HSBC, another large bank, are not likely to deter bad behavior.[301] For large firms, as lawyers and industry told Stimson, the factors ensuring compliance in general were: fear of being denied permission to export, fear of not being allowed to compete for federal contracts, fear of being personally held liable and criminally prosecuted (with jail time), and desire to have a good reputation to ensure good business and government relationships, and a larger, patriotic interest in national security.[302]

Small and foreign firms have similar challenges. Small firms face compliance challenges of: not knowing the laws and regulations involved (as noted earlier) or not feeling they can or need to afford to care about the complex laws and regulations involved.[303] In the 2013 COAC Export Survey, industry responses highlighted the fact that while large exporters are "well-versed" in export controls and requirements, many small sized exporters are not.[304] More so, foreign firms may not know they are even within the reach of US law and regulations[305] or will calculate that the cost of certain actions where they have little potential profit is not worth the risk of US enforcement actions.[306]

The US government, however, has wide latitude to undertake investigations and start inquiries or enforcement actions. Without clear government standards for compliance, companies have wondered, "How much compliance is enough?"[307] This applies to all legal and regulatory regimes, from the Foreign Corrupt Practices Act to fair employment practices to end-user verifications for sales under export controls.

Government does provide some guidance. Agencies from the Food and Drug Administration to the Occupational Safety & Health Administration have compliance guidance. The Department of Justice and the Securities and Exchange Commission (SEC) worked together to develop extensive guidance for compliance with the Foreign Corrupt Practices Act, which has been notoriously difficult for companies to manage.[308] Industry welcomed this extensive tome of interpretations of cases. However, in addition to this enhanced clarity, industry has pressed for reforms such as certain limitations on successor liability in acquisitions — an issue in general in most compliance areas, including export control and sanction violations.[309]

Related directly to export licensing and sanctions, government agencies do provide some guidance on compliance with laws and regulations. For example, BIS provides a list of red flag indicators to discover possible violations of EAR,[310] and DHS Project Shield provides training and outreach to export companies regarding proper protocol and requirements.[311] In addition to red-flag guidance, State, Commerce and Treasury release watch lists to assist industry determine whether they can export to certain individual end-users or companies, including the Arms Export Control Act Debarred List, the Entity List, and OFAC's US Specially Designated Nationals List.[312] A website managed by the International Trade Administration is meant to be a one-stop shop for assisting exporters in understanding all the requirements. However, it can be overwhelming to consider all the steps that a company has to go through to determine what its US obligations are for exporting, as well as all its obligations under the importing country's regulations.[313]

If an exporter violates export controls, sanctions or other requirements, it and those facilitating those actions bear the responsibility for that violation. The violations are considered part of

"strict liability" regimes. As noted earlier, penalties for violations vary — punitive action includes both administrative and criminal penalties. Administrative punitive actions include fines, revocation and suspension of export licenses and government contracts, and export denial. Criminal punitive actions include not only much higher levels of fines but also possible imprisonment. For sanctions, the Treasury Department's Office of Foreign Assets Control (OFAC) notes it has enforcement options that extend from taking no action to issuing a cautionary letter to a finding of a violation to levying civil penalties to initiating a criminal referral. The counterespionage section of the National Security Division of the DOJ supervises the investigation and prosecution of cases of export violation involving defense and sensitive exports — and it, like other government divisions, has much latitude in its decisions. Companies noted the wide latitude agencies have exercised in interpreting and enforcing export and sanctions violations.[314]

Federal sentencing guidelines for penalties also offer latitude that judges do take.[315] The guidelines look for mitigating factors including "an effective compliance and ethics program" and self-reporting of violations. Does a violation mean a compliance program is not effective? Law firms suggest that companies take a risk-based approach and note that such programs should be "*reasonably* designed, implemented, and enforced so that the program is *generally effective* in preventing and detecting criminal conduct."[316]

Given the complexity of compliance, firms may err in their operations and violate a control or sanction. The costs in time and money can quickly become high for the firm, especially when outside legal counsel is employed. This has become a center of expertise and business revenue for many law firms.[317]

---

[188] For a general overview of shipping terms, see: *Shipping and Incoterms*. New York: United Nations Development Programme Practice Series, November 2008. Accessed April 30, 2014. http://www.undp.org/content/dam/undp/documents/procurement/documents/UNDP-Shipping-Guide.pdf.

[189] Langley, John, Jr. *2014 Third-Party Logistics Study: The State of Logistics Outsourcing.* Paris: Capgemini Consulting, 2014. Accessed January 22, 2014. http://www.es.capgemini.com/resource-file-access/resource/pdf/3pl_study_report_web_version.pdf.

[190] Commonwealth of Pennsylvania. Department of Environmental Protection. *General Information Form -- Authorization Application NAICS Codes*. June 2002. Accessed February 10, 2014. http://www.dep.state.pa.us/dep/subject/advcoun/oil_gas/2003/05_GIF_NAICS_Codes1.pdf.

[191] US International Trade Commission (USITC). *Small and Medium-Sized Enterprises: Overview of Participation in US Exports*. January 2010. Accessed January 23, 2014. http://www.usitc.gov/publications/332/pub4125.pdf.

[192] DOC. Census Bureau. Foreign Trade Division *US Trade in Goods - Balance of Payments (BOP) Basis vs. Census Basis*. June 2013. Accessed January 28, 2014. http://www.census.gov/foreign-trade/statistics/historical/goods.pdf.

[193] United States Government. *Cross Agency Priority Goals: Exports*. Washington DC: Performance.gov, 2013. Accessed January 29, 2014. http://goals.performance.gov/node/38576. White House. *Cross Agency Priority Goals: Exports*. By Atkinson, Caroline. 2013. Accessed July 29, 2014. http://archive-goals.performance.gov/sites/default/files/images/Exports_CAP_Goal_FY2013_Q4_Update.pdf.

[194] DOC. Economics and Statistics Administration. *Recent US Export Trends and Foreign Economic Growth*. By Yu, Fenwick. April 22, 2014. Accessed April 29, 2014. http://www.esa.doc.gov/Blog/2014/04/22/recent-us-export-trends-and-foreign-economic-growth. This isn't really a report, which is how it's presently cited. I would probably change it to: Yu, Fenwick. "Recent US Export Trends and Foreign Economic Growth." April. 2014. ESA Blog. Last modified April 22, 2014. Accessed July 29, 2014. http://www.esa.doc.gov/Blog/2014/04/22/recent-us-export-trends-and-foreign-economic-growth.

[195] DOC. BIS. *Annual Report to Congress for Fiscal Year 2013.*

[196] These items may or may not be exported in the year they are granted a license, which are valid for two years. Licenses for crude oil are valid for one year. Author interview with DOC official. Washington, DC. April 22, 2014.

[197] DOC. BIS. *Annual Report to Congress for Fiscal Year 2012.* Accessed November 14, 2013. http://www.bis.doc.gov/index.php/forms-documents/doc_view/683-bis-annual-report-fy-2012.

[198] Bromley, Mark. "The Financial Value of States' Arms Exports." In *SIPRI Yearbook 2013: Armaments, Disarmaments and International Security,* 241-282. Oxford: Oxford University Press, 2013.

[199] USITC. *Recent Trends in US Services Trade, 2013 Annual Report*, 32. July 2013. Accessed April 29, 2014. http://www.usitc.gov/publications/332/pub4412.pdf.

[200] USITC. *Recent Trends in US Services Trade, 2012 Annual Report*, 31. July 2012. Accessed April 29, 2014. http://www.usitc.gov/publications/332/pub4338.pdf.

[201] USITC, *Small and Medium-Sized Enterprises*, IX.

[202] DOC. Census Bureau. *Preliminary Profile of US Exporting Companies, 2012.* December 2013. Accessed February 10, 2014. http://www.census.gov/foreign-trade/Press-Release/edb/2012/2012prelimprofile.pdf.

[203] DOC. "Shipping Your Product." November 2012. Accessed January 20, 2014. http://export.gov/basicguide/eg_main_043096.asp.

[204] Law Offices of George R. Tuttle. "US Controls On The Export And Re-export Of US Origin Goods & Technology - Commodity Jurisdiction." Trade Library. Accessed January 20, 2014. http://www.tuttlelaw.com/subjects/us_control_exp_re-exp_orig_of_tech/us_control_exp_re-exp_orig_of_tech_cj.html.

[205] DOC. BIS. "What is a Commodity Jurisdiction request and when and how do I submit one?" Commodity Jurisdiction. Accessed January 19, 2014. http://www.bis.doc.gov/index.php/licensing/commerce-control-list-classification/commodity-jurisdiction; DoS. Directorate of Defense Trade Controls. "Commodity Jurisdiction." http://pmddtc.state.gov/commodity_jurisdiction/index.html.

[206] "Violations and Penalties." *Code of Federal Regulations*, title 22, §127.

[207] "No person may order, buy, remove, conceal, store, use, sell, loan, dispose of, transfer, transport, finance, forward, or otherwise service, in whole or in part, any item exported or to be exported from the United States, or that is otherwise subject to the EAR, with knowledge that a violation of the EAA, the EAR, or any order, license or authorization issued thereunder, has occurred, is about to occur, or is intended to occur in connection with the item." "Enforcement and Protective Measures: Violations." *Code of Federal Regulations*, title 15, §764.2.

[208] US Treasury. Office of Foreign Assets Control. *Ask the TIC: Guide to Export Controls*. Trade Information Center. Accessed January 28, 2014. http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/tic-exp.pdf.

[209] US Treasury. *OFAC Regulations for Exporters and Importers*. January 2012. Accessed January 19, 2014. http://www.treasury.gov/resource-center/sanctions/Documents/facei.pdf.

[210] DoJ. Office of Public Affairs. "HSBC Holdings Plc. and HSBC Bank USA N.A. Admit to Anti-Money Laundering and Sanctions Violations, Forfeit $1.256 Billion in Deferred Prosecution Agreement." Justice News. Briefing Room. Last modified December 11, 2012. Accessed April 8, 2014. http://www.justice.gov/opa/pr/2012/December/12-crm-1478.html.

[211] DoS. Office of the Spokesperson. "State Department Announces Resolution of Raytheon Company Arms Export Control Enforcement Case." Press Releases: April 2013. Last modified April 30, 2013. Accessed April 8, 2014. http://www.state.gov/r/pa/prs/ps/2013/04/208655.htm.

[212] Reynolds, Tom. "Four Lessons from the Raytheon ITAR Violations." Export Solutions Inc., May 15, 2013. Accessed April 8, 2014. http://www.exportsolutionsinc.com/blog/four-lessons-from-the-raytheon-itar-violations/.

[213] DoS. Office of the Spokesperson. "State Department Announces Resolution of Raytheon Company Arms Export Control Enforcement Case."

[214] Ibid.

[215] United Technologies. "United Technologies Announces Resolution of Export Control Matters." News: News Center. Last modified June 28, 2012. Accessed April 30, 2014. http://www.utc.com/News/News-Center/Pages/United-Technologies-Announces-Resolution-of-Export-Control-Matters.aspx.

[216] Ibid.

[217] SMEs are companies with fewer than 500 full-time employees. Organization for Economic Co-operation and Development. "Small And Medium-Sized Enterprises (SMES)." Glossary of Statistical Terms. Last modified December 2, 2005. Accessed January 13, 2014. https://stats.oecd.org/glossary/detail.asp?ID=3123.

[218] USITC. *Small and Medium-Sized Enterprises: US and EU Export Activities, and Barriers and Opportunities Experienced by US Firms*, 332-509. July 2010. Accessed January 17, 2014. http://www.usitc.gov/publications/332/pub4169.pdf. XV-XX.

[219] USITC. *Trade Barriers that US Small and Medium-Sized Enterprises Perceive as Affecting Exports to the European Union*. March 2014. Accessed April 7, 2014. http://www.usitc.gov/publications/332/pub4455.pdf.

[220] For specific issues and recommendations from the Business Coalition for Transatlantic Trade regarding smaller firms' costs for standards compliance, see: USITC. *Trade Barriers that US Small and Medium-Sized Enterprises Perceive as Affecting Exports to the European Union*.

[221] United States Government. *Cross Agency Priority Goals: Exports*. Washington, DC: Performance.gov, 2013. Accessed January 29, 2014. http://goals.performance.gov/node/38576; White House. *Cross Agency Priority Goals: Exports*. By Atkinson, Caroline. 2013. Accessed July 29, 2014. http://archive-goals.performance.gov/sites/default/files/images/Exports_CAP_Goal_FY2013_Q4_Update.pdf.

[222] Export-Import Bank of the United States. "Expanding Your Exports: What Do You Need to Do?" Small Business Customers. Small Business. Accessed January 17, 2014. http://www.exim.gov/smallbusiness/smallbuscust/Expanding-Your-Exports.cfm.

[223] USITC, *Trade Barriers that US Small and Medium-Sized Enterprises Perceive as Affecting Exports to the European Union*, IX.

[224] DoJ. *Summary of Major US Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases.* March 2014. Accessed April, 30, 2014. http://www.justice.gov/nsd/docs/export-case-fact-sheet-201403.pdf. 18.

[225] While it is expected there will be a higher profit margin for re-exporting due to transportation costs, according to the Center for Global Development, the price differential is larger than should be expected. See Cobham, Alex, Petr Jansky, and Alex Prats. *Estimating Illicit Flows of Capital via Trade Mispricing: A Forensic Analysis of Data on Switzerland*. Washington, DC: Center for Global Development, January 2014. Accessed February 17, 2014. http://www.cgdev.org/sites/default/files/Cobham-illicit-flows-switzerland_0.pdf.

[226] Commodities trading is a major sector in Switzerland. Current Swiss law allows commodities traders to keep much of their activities undisclosed. Berne Declaration (Ed.). *Commodities: Switzerland's Most Dangerous Business.* Zurich: Berne Declaration, 2011. October 20, 2014. http://www.ladb.ch/fileadmin/files/documents/Rohstoffe/commodities_book_berne_declaration_lowres.pdf.

[227] Cobham, Alex, Petr Jansky, and Alex Prats. *Estimating Illicit Flows of Capital via Trade Mispricing: A Forensic Analysis of Data on Switzerland*.

[228] DOC. BIS. "Deemed Exports." Accessed April 29, 2014. http://www.bis.doc.gov/index.php/policy-guidance/deemed-exports; "Scope of the Export Administration Regulations." *Code of Federal Regulations*, title 15, §734.

[229] "Definitions of Terms as Used in the Export Administration Regulations (EAR)." *Code of Federal Regulations*, title 15, § 772.1.

[230] DoJ. *Summary of Major US Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases,* 23.

[231] Langley, John, Jr. *2013 Third Party Logistics Study*. Paris: Capgemini Consulting, 2012. Accessed January 20, 2014. http://www.capgemini.com/resource-file-access/resource/pdf/2013_Third-Party_Logistics_Study.pdf. 7.

[232] It is important to note the distinction, or lack thereof, between 3PLs and 4PLs. One interpretation is that a 4PL is like a 3PL but with better integrated technical services, and is also "an integrator that assembles the resources, capabilities and technology of its own organization and other organizations to design, build and run comprehensive supply chain solutions." See Hinkelman, Edward G. *Dictionary of International Trade, 9th Edition*. Petaluma, CA: World Trade Press, 2010. 6.

[233] Customs-Trade Partnership Against Terrorism (C-TPAT). "Minimum Security Criteria: Third Part Logistics Service Providers (3PL)." Accessed July 30, 2014. http://www.cbp.gov/sites/default/files/documents/3pl_security_criteria_3.pdf.

[234] Langley, John, Jr. *2008 Third Party Logistics Study*. Paris: Capgemini Consulting, 2008. Accessed January 20, 2014. https://www.scl.gatech.edu/research/supply-chain/20083PLReport.pdf.

[235] Chopra, Sunil, Adrian Alonso, Lance Donenberg, Daniel Gamba, and David Vely. *Technical Note: Third-Party Logistics: Current Issues and World Wide Web Resources*. Chicago: Kellogg School of Management, 1996.

[236] DHS. CBP. "Third Party Logistics Providers 3PL." CTPAT Minimum Security Criteria and Guidelines. Cargo Security and Examinations. AT Ports of Entry. Border Security. Accessed January 20, 2014. http://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat/security-guidelines/third-party-logistics-providers. 2.

[237] Dechter, Brad. "3PL or Freight Forwarder: What's in a Name?" Inbound Logistics, June 2008. Accessed January 20, 2014. http://www.inboundlogistics.com/cms/article/3pl-or-freight-forwarder-whats-in-a-name/.

[238] Langley, John, Jr. *2014 Third Party Logistics Study*, 7.

[239] Business Dictionary. "Non Vessel Operating Common Carrier (NVOCC)." Accessed February 9, 2014. http://www.businessdictionary.com/definition/non-vessel-operating-common-carrier-NVOCC.html.

[240] Langley, John, Jr. *2014 Third Party Logistics Study*.

[241] Ibid., 4.

[242] O'Reilly, Joseph. "2013 3PL Perspectives: Drafting a Blueprint for Growth." Inbound Logistics, July 2013. Accessed Janaury 17, 2014. http://www.inboundlogistics.com/cms/article/2013-3pl-perspectives-drafting-a-blueprint-for-growth/. 6.

[243] Ibid., 1.

[244] Ibid., 6.

[245] Langley, John, Jr. *2014 Third Party Logistics Study*, 6.

[246] Ibid.

[247] National Customs Brokers & Forwarders Association of America, Inc. (NCBFFA). *USPPI Responsibility Information Sheet.* Washington, DC: NCBFAA, January 2, 2014. Accessed July 29, 2014. http://www.ncbfaa.org/Scripts/4Disapi.dll/userfiles/uploads/USPPIExportResponsibilityInfoSheet52.pdf

[248] Langley, John, Jr. *2008 Third Party Logistics Study*, 30.

[249] Ibid., 29.

[250] Ibid., 32.

[251] Law Offices of George R. Tuttle. *Is C-TPAT Running Out of Steam?* San Francisco: Tuttle Law Offices, 2013. Accessed July 30, 2014. http://www.tuttlelaw.com/newsletters/2013/is_c-tpat_running_out_of_steam.html.

[252] DHS. CBP. "Third Party Logistics Providers 3PL."

[253] Customs-Trade Partnership Against Terrorism (C-TPAT). "Minimum Security Criteria: Third Part Logistics Service Providers (3PL)."

[254] Ibid.

[255] Ibid.

[256] Ibid.

[257] Seventy percent of those surveyed were small and medium sized logistics service providers.

[258] DHS. CBP. Advisory Committee on the Commercial Operations of Customs and Border Protection (COAC). *Export Survey*. 2013. Accessed April 7, 2014. http://www.cbp.gov/sites/default/files/documents/23%200%20COAC%202013%20Export%20Survey%20Report%20FINAL.pdf.

[259] Pengelly, Pamela D. *The "Q & A" On Freight Forwarders: Who Are They? What Do They Do? When Are They Liable?* Toronto: Cozen O'Connor, 2007. Accessed January 20, 2014. http://www.jdsupra.com/legalnews/the-q-a-on-freight-forwarders-who-a-66995/.

[260] Liability of Carriers under Receipts and Bills Lading. 49 US Code §14706.

[261] Primus, Brent. "Logistics and the Law: Freight claims in plain English." Logistics Management, July 1, 2012. Accessed March 3, 2014. http://www.logisticsmgmt.com/article/logistics_and_the_law_freight_claims_in_plain_english.

[262] Pengelly, Pamela D. *The "Q & A" On Freight Forwarders,* 2.

[263] Qualified Carriers. "Direct Liability & the Independent Tort of Negligent Hiring." Why You Need Us. Accessed February 10, 2014. https://www.qualifiedcarriers.com/negligent-hiring.aspx; Primus, Brent. "Logistics and the Law: Freight claims in plain English." Logistics Management, July 1, 2012. Accessed March 3, 2014. http://www.logisticsmgmt.com/article/logistics_and_the_law_freight_claims_in_plain_english. 48.

[264] DOC. BIS. *Don't Let This Happen to You: An Introduction to US Export Control Law*, 39. September 2010. Accessed April 30, 2014. https://www.bis.doc.gov/index.php/forms-documents/doc_view/535-don-t-let-this-happen-to-you-2010.

[265] Steptoe and Johnson LLP. "International Law Advisory - DHL Settles Export and Sanctions Charges in Exchange for 9.4 Million Dollars and an Audit Requirement." Publications. Last modified August, 7 2009. Accessed April 30, 2014. http://www.steptoe.com/publications-6280.html.

[266] DOC. BIS. *Texas Company to Pay $100 Million for Export Violations to Iran, Syria, Cuba, and Other Countries*. Last modified November 26, 2013. Accessed April 30, 2014. http://www.bis.doc.gov/index.php/about-bis/newsroom/press-releases/102-about-bis/newsroom/press-releases/press-releases-2013/603-texas-company-to-pay-100-million-for-export-violations-to-iran-syria-cuba-and-other-countries; US Treasury. *Weatherford International Ltd. Settles Potential Civil Liability for Apparent Violations of Multiple Sanctions Program*. November 26, 2013. Accessed April 30, 2014. http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20131126_weatherford.pdf.

[267] Author interviews with industry representatives.

[268] Michael Mullen, Executive Director of the Express Association of America, underscores the consequences of failing to appreciate distinct business models: "The division of the international logistics system into four 'modes' — air, sea, rail and truck — is overly simplistic and creates operational inefficiencies. There are at least three air cargo business models and possibly more." See: Congress. House. *Testimony of Michael C. Mullen: Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security*. 113th Cong., 1st sess., April 11, 2013. Accessed January 27, 2014. http://docs.house.gov/meetings/HM/HM07/20130411/100567/HHRG-113-HM07-Wstate-MullenM-20130411.pdf.

[269] Ruhal, Sanjeet. "High seas high-ways: Safety and security." *Journal of Law and Conflict Resolution* 5, no. 1. (January 2013): 1. Accessed July 30, 2014. http://academicjournals.org/article/article1379863290_Ruhal.pdf.

[270] NATS. "US Merchandise Trade with Canada and Mexico by Mode of Transportation (Tonnage) (Thousands of metric tons)." Section 6: North American Merchandise Trade. Tables. Last modified December 5, 2013. Accessed January 27, 2014. http://nats.sct.gob.mx/english/go-to-tables/table-6-north-american-merchandise-trade/table-6-2c-u-s-merchandise-trade-with-canada-and-mexico-by-mode-of-transportation-tonnage/#.

[271] Ibid.

[272] DoT. Research and Innovative Technology Administration. Bureau of Transportation Statistics. *Freight Transportation: Global Highlights.* 2010. Accessed April 30, 2014. https://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/freight_transportation/pdf/entire.pdf.

[273] US Treasury. Office of Foreign Assets Control. "Cuba: What You Need to Know About the US Embargo." Last modified January 2012. Accessed April 9, 2014. http://www.treasury.gov/resource-center/sanctions/Programs/Documents/cuba.txt.

[274] The International Convention for the Prevention of Pollution from Ships (MARPOL). United Nations Treaty Series 1340. February 17, 1978.

[275] Liability of Rail Carriers under Receipts and Bills Lading. 49 US Code §14706.

[276] Liability of Rail Carriers under Receipts and Bills of Lading. 49 US Code §11706.

[277] Liability of Rail Carriers under Receipts and Bills of Lading.49 US Code §14706.

[278] COGSA was developed from the Hague Rules, but increased the amount that carriers must pay exporters and importers for damage or loss of cargo. See: Ship Inspection. "Carriage of Goods by Sea Act 1936." Accessed February 10, 2014. http://www.shipinspection.eu/index.php/home/k2-item-view/item/183-carriage-of-goods-by-sea-act-1936.

[279] Dugan, Albert. *Limitation of Liability of Carriers by Sea and by Land*, 3. Philadelphia: Cozen and O'Connor, 2000. Accessed April 30, 2014. http://www.cozen.com/admin/files/publications/dugan204880.PDF.

[280] Ibid., 3.

[281] Liability of Water Carriers. 46 US Code §307.

[282] These include:

(a) act, neglect, or default of the master, mariner, pilot or the servants of the carrier in the navigation or in the management of the ship;

(b) fire, unless caused by the actual fault or privity of the carrier;

(c) perils, dangers and accidents of the sea or other navigable waters;

(d) act of God;

(e) act of war;

(f) act of public enemies;

(g) arrest or restraint of princes, rulers or people, or seizure under legal process;

(h) quarantine restrictions;

(i) act or omission of the shipper or owner of the goods, his agent or representative;

(j) strikes or lock-outs or stoppage or restraint of labour from whatever cause, whether partial or general;

(k) riots and civil commotions;

(l) saving or attempting to save life or property at sea;

(m) wastage in bulk or weight or any other loss or damage arising from inherent defect, quality or vice of the goods;

(n) insufficiency of packing;

(o) insufficiency or inadequacy of marks;

(p) latent defects not discoverable by due diligence;

(q) any other cause arising without the actual fault and privity of the carrier, or without the fault or neglect of the agents or servants of the carrier, but the burden of proof shall be on the person claiming the benefit of this exception to show that neither the actual fault or privity of the carrier nor the fault or neglect of the agents or servants of the carrier contributed to the loss or damage.

Protocol to Amend the International Convention for the Unification of Certain Rules of Law Relating to Bills of Lading (Visby Rules). United Nations Treaty Series 1412. February 23, 1968.

[283] Unless the air carrier can show exception through five common law exceptions. See DoT. *Cargo Liability Study*, 12. August 1998. Accessed April 30, 2014. http://ntl.bts.gov/lib/22000/22900/22922/cargolivab.pdf.

[284] Convention for the Unification of Certain Rules Relating to International Carriage by Air (Warsaw Convention). United Nations Treaty Series 137. October 12, 1929.

[285] DoT. *Cargo Liability Study,* 12.

[286] US Treasury. *Maersk Line, Limited Settles Sudanese Sanctions Regulations and Iranian Transactions Regulations Allegations*. July 2010. Accessed April 30, 2014. http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/07292010.pdf.

[287] Epstein, Jonathan, and Bobby Butler. "Complying with US Economic Sanctions, Export Controls and Anti-Corruption Laws in Aircraft Transactions and Flight Operations." Presented at the 65th Annual meeting for the National Business Aviation Association, October 30-November 1, 2012. Accessed March 3, 2014. http://www.nbaa.org/events/amc/2012/news/presentations/1031-Wed/NBAA2012-1031-complying-with-us-economic-sanctions-export-controls-anti-corruption-laws.pdf.

[288] Maleske, Melissa. "OFAC's global reach." Inside Counsel, July 31, 2012. Accessed April 30, 2014. http://www.insidecounsel.com/2012/07/31/ofacs-global-reach?page=2.

[289] Sherman, Rexford. *Seaport Governance in the United States and Canada*. Alexandria, VA: American Association of Port Authorities. Accessed April 11, 2014. http://www.aapa-ports.org/files/pdfs/governance_uscan.pdf.

[290] Sherman, Rexford. *Seaport* Governance in the United States and Canada. Alexandria, VA: American Association of Port Authorities. Accessed April 11, 2014. http://www.aapa-ports.org/files/pdfs/governance_uscan.pdf. Ibid.

[291] Ibid.

[292] Marine Terminal Operator; Schedule of Rates, Regulations and Practices. Anchorage, AK: North Star Terminal & Stevedore Co., LLC, July 2008. 19.

[293] Marine Terminal Operator; Schedule of Rates, Regulations and Practices. Anchorage, AK: North Star Terminal & Stevedore Co., LLC, July 2008. 19. Ibid.

[294] However, the reality of liability, especially concerning negligence, is often decided in courts. For example, the Port Authority of New York and New Jersey was deemed liable for 1993 World Trade Center bombing by a jury in 2008. However, this initial verdict was overturned, highlighting the uncertainty with issues of negligence regarding port areas. See Hartocollis, Anemona. "Port Authority Liable in 1993 Trade Center Attack." The New York Times, April 30, 2008. Accessed April 30, 2014. http://www.nytimes.com/2008/04/30/nyregion/30bombing.html?pagewanted=all; Marine Terminal Operator; Schedule of Rates, Regulations and Practices. Anchorage, AK: North Star Terminal & Stevedore Co., LLC, July 2008. 19. Second one was cited in immediately preceding footnote. Would do: Marine Terminal Operator; Schedule of Rates, Regulations and Practices, 19.

[295] Marine Terminal Operator; Schedule of Rates, Regulations and Practices, 16.

[296] Ibid., 33.

[297] US Treasury. *General Reinsurance Corporation Settles Iranian Transactions Regulations Allegations*. June 2011. Accessed May 1, 2014. http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/06292011.pdf.

[298] US Treasury. "Sanctions Frequently Asked Questions and Answers." Resource Center. Last modified April 14, 2014. Accessed May 3, 2014. http://www.treasury.gov/resource-center/faqs/Sanctions/Pages/answer.aspx#global1.

[299] International Chamber of Commerce (ICC). "The new Incoterms 2010 rules." Tools for trade. Products and Services. Accessed April 30, 2014. http://www.iccwbo.org/products-and-services/trade-facilitation/incoterms-2010/.

[300] Freifeld, Karen, Aruna Viswanatha, and David Henry. "JPMorgan agrees $13 billion settlement with US over bad mortgages." Reuters, November 19, 2013. Accessed April 30, 2014. http://www.reuters.com/article/2013/11/20/us-jpmorgan-settlement-idUSBRE9AI0OA20131120.

[301] Sledge, Matt. "HSBC Gets Small Fine for Terrorist Transactions." Huffington Post, December 18, 2013. Accessed April 30, 2014. http://www.huffingtonpost.com/2013/12/18/hsbc-terrorists_n_4467329.html; Viswanatha, Aruna and Brett Wolf. "HSBC to pay $1.9 billion US fine in money-laundering case." Reuters, December 11, 2013. Accessed April 30, 2014. http://www.reuters.com/article/2012/12/11/us-hsbc-probe-idUSBRE8BA05M20121211.

[302] Interviews with industry members and lawyers by author.

[303] Interviews with industry members by author.

[304] DHS. CBP. Advisory Committee on the Commercial Operations of Customs and Border Protection (COAC), 36.

[305] Maleske, Melissa. "OFAC's global reach."

[306] Worstall, Tom. "HSBC's $1.9 Billion Money Laundering Fine and the Somalian Cost of Bank Regulation." Forbes, August 8, 2013. Accessed April 30, 2014. http://www.forbes.com/sites/timworstall/2013/08/08/hsbcs-1-9-billion-money-laundering-fine-and-the-somalian-cost-of-bank-regulation/.

[307] Interviews with industry members by author.

[308] DOJ and US Securities and Exchange Commission (SEC). A Resource Guide to the US Foreign Corrupt Practices Act. November 2012. Accessed December 12, 2013. http://www.justice.gov/criminal/fraud/fcpa/guide.pdf.

[309] Foster, Dulce, and Lousene Hoppe. "Enforcing the Foreign Corrupt Practices Act: Guidance through a Glass, Darkly." Bench & Bar of Minnesota, March 11, 2013. Accessed January 17, 2014. http://mnbenchbar.com/2013/03/foreign-corrupt-practices-act/.

[310] DOC. BIS. "Red Flag Indicators." Accessed April 28, 2014. http://www.bis.doc.gov/index.php/enforcement/oee/compliance/23-compliance-a-training/51-red-flag-indicators.

[311] DoS. "Red Flags and Watch Lists." Accessed April 28, 2014. http://www.state.gov/strategictrade/redflags/.

[312] Ibid.

[313] Export.gov. "Export Licenses, Standards and Economic Sanctions." Licenses & Regulations. Last modified February 15, 2013. Accessed January 16, 2014. http://export.gov/regulation/index.asp.

[314] Interviews with industry members by author.

[315] Lind, Dara. "Judges are Following Sentencing Guidelines Less Than Half the Time." Vox, May 7, 2014. Accessed May 12, 2014. http://www.vox.com/2014/5/7/5690982/judges-are-following-sentencing-guidelines-less-than-half-the-time.

[316] Marks, Norman. "Assessing Internal Controls Over Compliance Risks." InternalAuditor Blog, October 23, 2012. Accessed February 5, 2014. http://www.theiia.org/blogs/marks/index.cfm/post/Assessing%20Internal%20Controls%20Over%20Compliance%20Risks; Baker & McKenzie. "Global Corporate Compliance." Accessed July 31, 2014. http://www.bakermckenzie.com/globalcorporatecompliance/.

[317] See, for example, Vinson & Elkins Law. "Export Controls and Economic Sanctions." International. Practices. Accessed May 7, 2014. http://www.velaw.com/practices/ExportControlsEconomicSanctions.aspx; Perkins Coie LLP. "Export Controls." Practices. Accessed May 7, 2014. http://www.perkinscoie.com/export_controls/.

Finding the Business Case for Security

While efficiency and security may seem like dueling goals in global trade, the two often can complement one another. Here we consider several factors that can shape opportunities for mutual advantage, along with some past and current efforts that illustrate some of the challenges.

Leveraging Technology for Trade Transparency

European and Asian port operations are more efficient than elsewhere in several key respects. The advantage owes largely to automation technology and the development of "smart ports,"[318] which aim to increase berth productivity while ensuring the secure transfer of goods. American ports, however, are beginning to implement automation technology. Long Beach, California, is constructing a "smart harbor" at Middle Harbor, aiming to increase container lifts per hour by 50 percent while reducing operation costs.[319] The modernized terminal is due to be completed by 2020 at a cost of over $1 billion.[320]

Port productivity, however, is not just a function of berth and crane efficiency. When berths are able to process more containers, other terminal operations must make commensurate improvements in order to avoid bottlenecks.[321] More efficient trade flows are directly related to security outcomes, as they enable officials to focus more on higher-order risks. There is evidence that in some circumstances, these risk-segmentation benefits can be unlocked not just through technology, but also by deploying greater government resources. One recent study, for example, found that deploying one additional CBP primary inspection officer at port can increase GDP by $2 million.[322]

The US Federal Highway Administration is producing a congressionally mandated National Freight Strategic Plan, which will assess the country's "primary freight networks."[323] The document will map current and future bottlenecks for trade and highlight particular safety concerns. However, according to interviews conducted by the project team, the initiative to date has failed to adequately map intermodal areas.

Companies already have taken steps to implement end-to-end container tracking.[324] To achieve this goal, there is a need for more remote container tracking technology and "smart containers," especially in the transport of high value cargo.[325] Truck and ship tracking is already available,[326] but specific container tracking and sensing technology is still in the development phase.[327]

Track-and-trace technology is used to log and provide information in real time on geo-position of containers, as well as to relay information on container conditions through sensor technology. Acquisition of remote container tracking has increased steadily in recent years. The number of remote container trackers on intermodal containers rose from 89,000 in 2011, to 137,000 in

2012.[328] By 2017, the number of remote trackers could rise above 1 million.[329] Overall, these advances have helped increase efficiency of the supply chain, providing data for automated data acquisition and information sharing, as well as improving supply chain knowledge for better management.[330]

Whether in the supply chain domain or elsewhere, making data actionable – particularly when many parties are involved – depends on a shared understanding of ends, ways and means.[331] For example, industry is often concerned about government and private sector competitors gaining access to proprietary information, as well as the costs of providing this information. The Transportation Research Board has identified motivators for industry to share non-restrictive data, including funding opportunities to cover the costs of data-sharing, as well as assurances the data will be properly "scrubbed" and not used for regulatory enforcement purposes.[332]

Another facilitator in some contexts could be the designation of a trusted third-party agent to safeguard and analyze shared information.[333] A government-backed precedent for sharing proprietary information already exists in the "protected critical infrastructure information" (PCII) model. The Transportation Research Board suggests that government provide a clearer explanation of how it uses such data in similar programs.

In terms of information exchange at the border, there is increasing emphasis on both automation and more efficient provision of vital and relevant information, thereby creating a single-window system for reporting imports and exports to the government. CBP has placed an emphasis on ensuring automation, including requiring that all import and export documents be filed through the Automated Commercial Environment (ACE) by May 2015. Under the Security and Accountability for Every Port Act of 2006, Congress requires the Secretary of the Treasury to oversee a CBP-operated single portal system, the International Trade Data System (ITDS), which currently comprises 48 US government agencies in a federated clearinghouse through which trade entities can submit required.[334]

CBP is moving toward electronic export manifests across all modes of transport, and evaluating the best system for submitting these manifests, including continuing to pursue the Export Manifest pilot currently underway that allows for electronic submission and automated processing for ocean carriers over the coming year.[335] Currently, the information that importers provide to the US government falls into four categories: product identification, product characterization, product description, and dictionary and catalogue.[336] However, the usefulness of descriptions is questionable, and the often-delayed exchange of information can create problems in an industry where threats move quickly. Thus far the Export Manifest pilot has been successful in improving data collection efficiency and in lowering costs.

As part of the Advance Manifest Rules, importers are required to file data on incoming cargo to CBP via an electronic data interchange system. Specific deadlines depend on the mode of transport.

For imports into the US, ocean vessels must submit information at least before 24 hours before lading for non-bulk shipments and at least 24-hours before arrival bulk-shipments. Under the Importer Security Filing ("10+2") requirements, importers must provide information on the seller, buyer, importer of record number, consignee number, manufacturer, ship to party, country of origin, the Commodity Harmonized Tariff Schedule of the United State number,[337] and a stow plan of containers onboard.[338] Rail importers must submit information two hours

before arrival into the US. Truck importers are required to submit information one hour before arrival at the border if they are not part of FAST, and 30 minutes before if they are part of FAST. In terms of air cargo, for imports from NAFTA countries or Central American and South American countries above the Equator, carriers are required to submit cargo manifests four hours before "wheels up."[339]

There are several voluntary/pilot programs to provide benefits to US importers/exporters that submit shipment and commodity data. Under the Advance Export Information pilot, for example, US exporters provide export information to the Commerce Department on an expedited timeline (see table below). Under the Air Cargo Advance Screening (ACAS) pilot, carriers submit information on US-bound cargo at the earliest point possible prior to loading.[340]

Filing Times for Participants in Advance Export Information Pilot

	USML Shipments	Non-USML Shipments (Including CCL Items)
Vessel Cargo	24 hours prior to scheduled vessel departure from United States	24 hours prior to loading cargo at United States port
Air Cargo	8 hours prior to scheduled departure from United States	2 hours prior to scheduled departure time from United States
Truck Cargo	8 hours prior to scheduled departure from United States	1 hour prior to the arrival at the United States border to be transported abroad
Rail Cargo	24 hours prior to scheduled train departure from United States	2 hours prior to the arrival at the United States border to be transported abroad

A major initiative to improve the overarching framework for the submission and use of trade data is the International Trade Data System (ITDS). If implemented fully and effectively, ITDS will help all government agencies with border management functions to standardize data required from industry.[341]

ITDS is made up of three components: the Participating Government Agency (PGA) Message Set, Interoperability Web Services (IWS), and Document Image System (DIS).[342] PGA creates a well-harmonized data set using importer declarations that are collected via DIS, which is transmitted to other agencies through the IWS. CBP is expediting the integration of ITDS into the Automated Commercial Environment, although this requires sustained momentum from US agencies and departments.[343]

Consumer Product Safety Commission ITDS/RAM Pilot Program for Imports

The Consumer Product Safety Commission (CPSC) is charged with protecting the public from unreasonable risks of injury or death associated with the use of the thousands of types of consumer products under the agency's jurisdiction." CPSC, utilizing the same technology and best practices as implemented by FDA's import team (the PREDICT system), was able to implement a risk assessment methodology to address all of the agency's pressures while optimizing its limited inspection resources. As a Participating Government Agency in CBP's International Trade Data System, CPSC is able to electronically access data on relevant imports in time to request holds on specific shipments at ports of entry. Using this interface, CPSC developed and implemented decision management processes and systems for identifying suspect products and requesting inspections through CBP.

Many of the products for which CPSC is responsible are imported into the US. The import volume is extremely large, consisting of over 14 million entry lines annually equating to over $600 Billion in value, disbursed across 327 ports and growing rapidly. However, CPSC's inspection resources are quite limited, with the ability to inspect only 0.05 percent of the import volume. CPSC is challenged with overseeing this large volume in the context of a constrained budgetary environment, as well as a need to balance ensuring that trade flowed efficiently as well as fulfill its mission to protect the public from unsafe consumer products.

The International Trade Data System-Risk Assessment Methodology ("ITDS/RAM" or "RAM"), blends analytics and business process optimization with cutting-edge technology to create a platform through which CPSC can exchange data with CBP; analyze transactional data for risk factors; aggregate findings into actionable recommendations; and capture feedback and outcomes to refine the decision making over time. Along with the interface to CBP through ITDS, the solution also supports CPSC in integrating data and activities across its focus areas of import compliance, domestic compliance, and safe manufacture through coordinated business processes, information technology, and resource alignment.

CPSC's ITDS/RAM enables industry to interact more efficiently with CBP as the central front-end trade information broker yet enables CPSC to fulfill its agency mission and leverage its institution-specific knowledge to optimally protect the public.

It is anticipated that the ITDS/RAM system will:

save lives and prevent injuries
The system is projected to prevent approximately 20 deaths and 20,000 injuries annually.

reduce recalls
Through improved targeting, high risk cargo will be stopped at ports of entry. Thus, the RAM will better protect companies and industries from the cost and legal exposure resulting from distribution and retail of products that are hazardous and may ultimately be subject to recall.

facilitate trade
By identifying lower risk importers and manufacturers who supply consistently compliant products into US commerce, CPSC can allow them reduced review at importation, resulting in a reduction in associated port processing and a savings of costs and time.

yield an overall economic return
The system is anticipated to provide a $546 million annual benefit to US consumers and industry, including manufacturers, importers and retailers.

The White House National Security Council created a task force to coordinate this process as a priority implementation task pursuant to the National Strategy for Global Supply Chain Security.[344] The information from ITDS has been leveraged by the Consumer Product Safety Commission (CPSC) through an integrated ITDS/Risk Assessment Methodology (RAM) Pilot program. ITDS/RAM allows shippers to submit information on imports that is funneled through the Risk Assessment Methodology (RAM) and combined with CBP data to identify import risks.[345] The US Food and Drug Administration uses PREDICT, a similar risk-based analysis system using data-mining, to identify tampered or illegal goods entering the US.[346]

In 2014, CBP is reengineering and modernizing the Automated Export System (AES) to roll out limited *export-related* functionality for ITDS. Capitalizing on this new functionality, the Census Bureau, in cooperation with CBP, is launching a voluntary Advance Export Information pilot. The pilot will seek to evaluate a new data-filing option in AES and will "help determine whether the advanced export information permits CBP to effectively screen exports and will help identify and mitigate risk with the least impact practicable on trade operations."[347] To enable automated validation of all export data, an interface will be developed between the USXPORTS system and the Automated Commercial Environment.[348]

To begin testing the "single window" functionality ITDS is meant to deliver, CBP in January 2014 launched a two-year pilot for processing a limited number of data elements that the Food Safety and Inspection Service and the Environmental Protection Agency require of US importers. The pilot aims to "enhance the interaction between international trade partners, CBP, and PGAs by facilitating electronic collection, processing, sharing, and review of trade data and documents required by Federal agencies during cargo import and export process."[349]

Industry has voiced concerns regarding the burden of data requirements. The American Association of Exporters and Importers, for instance, highlights the importance of "smart data," rather than simply collecting large amounts of data.[350] The trade association also has noted that participating government agencies must actively engage with private industry to stipulate what information is needed, depending on the nature of the threat.

Signed by President Obama in February 2014, Executive Order 13659 mandates several important trade facilitation measures.[351] It sets a deadline of December 31, 2016, for full deployment of ITDS across all participating agencies.[352] At that point, US exporters/importers will be able to transmit required trade data to government through a "single window" system.[353]

To ensure both interagency and industry involvement in improving ITDS, regulations and the improvement of supply chain management, the EO codifies and empowers a Border Interagency Executive Council (BIEC), chaired by DHS.[354] The BIEC will work with government agencies to streamline border management operations, including trade processing, and promote common approaches to risk management. To that end, relevant agencies must report to the ITDS Board of Directors on their use of international standards for product classification and identification.

As mandated by the EO, the BIEC also is engaging with industry to identify opportunities for greater supply chain efficiencies and enhanced enforcement. In a related outreach role, the BIEC will coordinate with other countries to encourage development of similar single-window systems.[355]

One issue that has emerged is whether ITDS data elements should be coordinated with international trading partners in order to better facilitate trade. On paper, the US government acknowledges the benefits of international standardization — including in terms of data requirements and formatting, noting, "Providing a platform for customs administrations to share information and providing advance notice of risky shipments could effectively extend the enforcement perimeter beyond US borders."[356] However, US government representatives have expressed security concerns over such data sharing.[357] The data set in ITDS only conforms "in part" to agreed WCO standards: "CBP has not yet undertaken steps to implement the WCO standard messages within ACE. Implementation has been notionally considered as a second reporting option, to be developed after other ACE functions are completed."[358]

STAKEHOLDER ENGAGEMENT

Government realizes the value of engaging the private sector — and others — as partners to achieve common goals. This is evident in some of the examples provided below for the ways that the US government has engaged with industry.

From reviewing stakeholder engagement efforts, Stimson found the following:

- The US Government has produced good guidance on outreach to the private sector.
- Broad engagement, including with the private sector, is maturing in certain areas of national security interest, particularly related to disaster planning and response and in critical infrastructure. However, communication and cooperation are still nascent in other areas of importance to national security.

Below, we first look at some general public-private models and the National Planning Frameworks, which have taken much public and private effort to develop. Finally, we consider industry engagement more directly related to trade and commerce.

GENERAL US GOVERNMENT ENGAGEMENT MODELS

The US government has created a variety of councils and committees in order to facilitate increased coordination between the public and private sectors. Most recently, Executive Order 13629 established the White House Homeland Security Partnership Council in 2012 as a means to facilitate partnerships between government and private sector actors, as well as NGOs, state, local, tribal and territorial governments and law enforcement agencies, to better address security issues. The Executive Order requires that the Council be chaired by the Assistant to the President for Homeland Security or a member of the National Security Staff.[359] The Council receives guidance on the scope of issues to be addressed and operational processes from an established Steering Committee, and members of the Council include designated federal nominees from agencies that are members of the Steering Committee. Primary functions of the Council include facilitating collaboration among various stakeholders in order to promote security priorities, collaborate with those actors interested in expanding local homeland security partnerships, and establishing annual meetings to discuss issues and best practices.[360]

The Department of State has also recognized the benefits of leveraging others' expertise and efforts. As part of its Global Partnership Initiative, it developed an excellent guide that describes

a range of models, including monetary, non-monetary and combined resource partnerships. The guide noted that while partnerships may take a variety of forms, they should all establish certain baselines, such as a memorandum of understanding containing information on the partner organizations, shared goals and objectives, and operating principles.[361]

In 2013, the National Security Council staff published a guide of best practices for building partnerships and included details on the different types of partnerships similar to those provided by the State Department. Intended for use by federal agencies, the guide notes that, among the variety of attributes that may be included within a given partnership, nine key elements lend to more successful collaborations. These include clear objectives and scope, early engagement, sufficient resources, mutual responsibility and benefits, trust and respect, communication and transparency, careful management, compliance with legal requirements, and mutual planning for implementation and evaluation.[362] The guide also provides insights on things federal agencies should be mindful of when developing a partnership, such as avoiding accusations of privileged access by issuing general requests for action to a wide audience and performing due diligence to avoid potential conflicts of interest.[363]

The Executive Branch has been reaching out beyond government for citizen input since the time of George Washington. To provide greater structure and transparency for these efforts, the 1972 Federal Advisory Committee Act set a formalized process of "establishing, operating, overseeing, and terminating" federal advisory committees. Under this act, the General Services Administration monitors compliance of the over 1000 federal advisory committees with FACA — providing a database of the advisory committees and increasing transparency. [364]

The Department of Homeland Security has many advisory committees and task forces, including the Homeland Security Advisory Council[365] made up of a diverse group of law enforcement, think tank leaders, former government leaders and a few industry reps.[366]A separate National Infrastructure Advisory Council (NIAC), appointed by the president, brings together a variety of stakeholders to provide the president, through the Secretary of DHS, advice specifically on critical infrastructure protection and has more corporate leaders on it.[367] It also can advise other agencies that have critical infrastructure responsibilities.[368] Leveraging expertise from top industry leaders, government agencies and academia, the NIAC is especially focused on improving information sharing and improving risk-management.

DHS has also established a Private Sector Office to coordinate increased dialogue with all types and levels within the private sector and inform the Secretary of Homeland Security on how relevant policies and regulations impact industry. One mechanism the Office established for increased collaboration between private industry and government is the Loaned Executive Program, in which private sector experts volunteer to work alongside DHS officials for an extended period. Participation in the program may last from three months to one year, with the potential for reappointment not to exceed a total of two years. Efforts to get the program off the ground were delayed due to legal provisions and restraints. As of December 2013, 13 total private sector executives had engaged in the program, and the Office hopes to extend participation to 20 executives by the end of fiscal year 2014.[369]

Notwithstanding its original goal, available information suggests that the Private Sector office has limited resources and uneven coordination with other DHS projects and programs. Even within DHS, many personnel are unaware of the program and the extent of its work,[370]

including the *Private Sector Resources Catalogue*, a guide to available industry training, regulation guidance and DHS services and programs for the public sector.[371]

Within DHS, the Federal Emergency Management Agency (FEMA) also relies extensively on public-private collaborations. It notes attributes for successful public-private partnerships, many of which highlight the importance of sharing information on situational awareness for emergency preparedness and response, and encourages public-private coordination to incorporate core attributes of being "publically accessible, dedicated resourced, engaged and sustainable" so as to provide benefits to whole communities.[372] The FEMA website lists a number of current public-private partnerships, ranging from national collaborations and regional or state-supported initiatives, to event-specific efforts.[373]

National Planning Frameworks

The National Planning Frameworks are the product of a lengthy multi-stakeholder collaboration that included a role for industry. Issued in 2011, Presidential Policy Directive 8 (PPD-8) mandated development of a National Preparedness Goal. As elaborated in the resulting DHS document, the Goal emphasizes strengthening the nation's security and resilience through whole-of-community preparation for threats and hazards that pose the greatest risk to US national security. To support these efforts, DHS also led development of National Planning Frameworks in five preparedness mission areas identified within PPD-8: prevention, protection, mitigation, response and recovery.

DHS broke down priority actions for meeting the National Preparedness Goal into 31 core capabilities, which in turn appear across the five planning frameworks. An example is intelligence/information sharing, which figures most prominently in the National Prevention Framework and the National Preparedness Framework. This capability calls on stakeholders to share timely and accurate information on threats to the US, WMD activity, and any other issues concerning US national security.[374] It also recommends that the various actors have access to mechanisms for submitting and receiving information related to terrorism and other suspicious activities.

The March 2013 National Preparedness Report highlights the national network of fusion centers and Joint Terrorism Task Forces as examples.[375] It must be noted, however, that regulators and the expert community at times have questioned the effectiveness of some of these mechanisms. For example, a report issued jointly by Democratic and Republican staff from the Senate Homeland Security and Government Affairs Committee found that the counterterrorism-focused fusion centers often did not effectively support timely or actionable threat information.[376]

On a more optimistic note, the Hurricane Sandy Rebuilding Task Force suggested industry participation in public-private partnerships. Established by executive order in December 2012 and chaired by the Secretary of Housing and Urban Development, the Task Force implemented a regional design competition to promote innovation for improving resilience, Rebuild by Design, which encourages industry experts to provide solutions to regional issues that may be too vast for any one community to address on its own.[377] Winning design solutions may then be supported by philanthropic and federal funding and implemented to assist the larger recovery

effort. This strategy works to bring a wide variety of government and industry experts together to promote restructure, recovery, and resilience in affected regions.

While the planning frameworks detail a number of measures the private sector may take to address the core capabilities, they do not provide much insight on ways to prioritize these activities for optimizing national preparedness. And despite their name, the National Planning Frameworks do not address broader US national security interests. Indeed, an unclassified summary of the Strategic National Risk Assessment – the document that provided an overarching structure "does not explicitly assess persistent, steady-state risks like border violations, illegal immigration, drug trafficking, and intellectual property violations, which are important considerations for DHS and the homeland security enterprise."[378]

It is clear that more — and better — planning is needed.

Public-Private Mechanisms Focused on Trade

In terms of sector-specific security, industry advisory committees have been formed to aid the executive branch and Congress on improving national security within the supply chain. For example, the National Maritime Security Advisory Committee (NMSAC) provides recommendations and advice on national maritime issues. It can establish Area Maritime Security Advisory Committees in any port in the United States, which recommendations to DHS and Congress on local maritime issues. The NMSAC is mandated to include representatives from facility owners, industry, and the local, state and national government.[379]

A variety of other trade-related advisory committees exist across the executive branch. These include the President's Export Council Subcommittee on Export Administration (PECSEA), the Regulations and Procedures Technical Advisory Committee (RPTAC), the Advisory Committee on Supply Chain Competitiveness (ACSCC), and the Advisory Committee on Commercial Operations of Customs and Border Protection (COAC).[380] The first three are sponsored by the Commerce Department, the fourth by CBP.

Information Sharing

While they can take many different forms, public-private partnerships often can be strengthened and made more sustainable through some type of information sharing arrangement.[381] Independent organizations such as the Markle Foundation have looked at ways that information can be best shared while protecting individual privacy and proprietary corporate information.[382]

From reviewing information-sharing efforts, the project team found the following:

- Information-sharing efforts are extensive and range from White House efforts, to congressional mandates, to agency and sector-specific plans. However, industry criticizes current information-sharing initiatives for being oriented more towards industry providing information to government agencies and in return not receive timely, actionable intelligence and for being uncoordinated across government — with industry not knowing the options or best places to engage but being visited by different government officials

who may be unaware of others' outreach. Too often, the private sector feels like it gives information may be subject to further investigation itself as a result.[383]

- Since much effort is devoted to engaging critical infrastructure stakeholders, public-private partnership efforts tend to be rather narrow in scope. The critical infrastructure model is one that can be better leveraged and adapted into broader areas of national security.
- Little effort has been devoted to identifying information not being shared that could be useful to partners and establishing ways to capture this information and reduce barriers to sharing. Progress is being made, particularly in the cyber area, but slowly given that the issue of information sharing has been discussed for many years.

Below we consider the government's strategic initiatives for information sharing and then look at some national security information-sharing efforts. We comment on the evolution of non-governmental information-sharing trends and services that have emerged to help develop and manage information needs; before we take an in-depth look at critical infrastructure's well-developed engagement, information-sharing and risk model in the next section.

GOVERNMENT DIRECTIVES ON INFORMATION SHARING

Effective information-sharing for transparency and risk management requires enhanced tools and processes that benefit both government and industry. Yet, it is important to note the differences between information-sharing as an end objective and information-sharing as a component of a larger collaborative effort between government and industry actors. The following examples of a few key programs are intended to highlight this difference, and lend to greater understanding of the multiple facets that encapsulate information-sharing processes.

National Strategy on Information Sharing and Safeguarding

The National Strategy on Information Sharing and Safeguarding, released in December 2012, stems from the 2010 National Security Strategy and builds on the 2007 National Strategy for Information Sharing. The 2012 Strategy is also, in part, a response to recommendations provided in a 2012 report from the National Infrastructure Advisory Council. The Strategy emphasizes the need to not only share pertinent information with authorized personnel who work to maintain national security, but also to safeguard that information from nefarious actors — a necessity that should be limited by existing laws and policies, and not by technology. The Strategy is guided by three main principles, namely to treat information as a national asset, to engage in shared risk management, and to make information discoverable and retrievable by authorized users so as to better inform decision-making.[384] These principles help shape the five main goals of the Strategy:

- Drive collective action through collaboration and accountability
- Improve information discovery and access through common standards
- Optimize mission effectiveness through shared services and interoperability
- Strengthen information safeguarding through structural reform, policy and technical solutions
- Protect privacy, civil rights, and civil liberties through consistency and compliance

As part of the way forward, the Administration defined the top five objectives to achieving the information sharing and safeguarding goals detailed in the Strategy. They include aligning information sharing and safeguarding governance to cultivate enhanced decision-making; developing guidelines for sharing and safeguarding agreements to address common requirements, including privacy, civil rights and liberties; adopting metadata standards to facilitate federated discovery, access, correlation and monitoring across Federal networks; extending and implementing the FICAM roadmap across all security domains; and implementing removable media policies, processes and controls to better detect, deter and disrupt insider threats.[385]

The Strategy highlights fusion centers as a major mechanism for sharing and receiving information among various actors. A 2013 study conducted by the Committee on Homeland Security noted that while the subcommittee believes the National Network of Fusion Centers will continue to grow and become increasingly valuable to both government and industry stakeholders, operational capacities within individual centers are lacking.[386]

Program Manager for the Information Sharing Environment (PM-ISE)

In 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act (IRTPA), which mandated the creation and implementation of an Information Sharing Environment (ISE). As noted in IRTPA, the ISE generally refers to "an approach that facilitates the sharing of terrorism information, which...may include any methods of determined necessary."[387] This is a broad environment that functionally incorporates five different communities — defense, intelligence, homeland security, foreign affairs, and law enforcement. These communities work to support the principal users of the information sharing environment.[388]

Through IRTPA, the President is required to select a Program Manager for the established ISE, otherwise known as the PM-ISE. This person is responsible for managing the development of standards, procedures, and best practices for the ISE at large. In this capacity, the PM-ISE brings together mission partners of the ISE and provides government-wide standards and procedures for the effective development, implementation, and operation of the ISE. The PM-ISE also collaborates with a variety of communities within the US to improve the discovery and sharing of information as it may pertain to counterterrorism, homeland security, and WMDs.

The PM-ISE seeks to engage industry stakeholders through standards-based innovation. While predominately centered on the owners and operators of critical infrastructure, the development of standardized business processes for information exchange reportedly allows various industry stakeholders to further participate in the ISE. However, as a recent PM-ISE presentation noted, this participation is underdeveloped, as sharing between private industry and government is not truly bi-directional.[389] Thus, a disparity remains between current and best practices for efficient and effective public-private information sharing.

In early 2014, the PM-ISE released an ISE Management Plan to coordinate business processes and collaboration among the various ISE stakeholders. The Management Plan notes that the overall goal is to combine information sharing efforts across government to expand implementation of the ISE and to promote more standardized policies and practices among partners.[390] The Management Plan offers details on the tools and resources available to assist stakeholders in sharing information as described in the ISE, and these details are organized

into four overarching categories: governance and policy, budget and performance, standards and interoperability, and communications. The ISE Interoperability Framework (I^2F) as detailed in the Management Plan provides a method for exchanging information across an array of information systems independently utilized by the various ISE stakeholders.

Suspicious Activity Reporting Initiative

In response to the growing need to standardize suspicious activity reporting, especially for terrorism, the US launched the Nationwide Suspicious Activity Reporting Initiative (NSI), a multi-agency effort to create a standardized process for identifying and reporting suspicious activity.[391] The overall goal of NSI is to ensure that no matter where a suspicious activity is reported, the information will be easily and readily shared across the entire nation with all relevant agencies.[392]

The NSI is a three-pronged effort to increase suspicious activity reporting and improve the processing of submitted information. First, the FBI's eGaurdian system, a secure but unclassified network, was leveraged as a common platform for submitting suspicious activity reports, commonly called SARs. Other participating agencies (including DoD, DHS, and DoJ) and local and state law enforcement can easily submit received information through the system, overcoming compatibility issues.

Second, the NSI works to raise awareness through a variety of training programs with non-law enforcement constituencies (hometown security partners), including those charged with protecting the nation's critical infrastructure.[393] For example, in 2013 NSI increased its outreach to the maritime industry through the Maritime Suspicious Activity Reporting Initiative, partnering with the US Coast Guard and Maritime Intelligence-Integration Office to educate ports and maritime supply chain stakeholders on suspicious activity reporting.[394]

And third, NSI has made collated submitted information available to constituents with Roll Call Release products that highlight emerging security issues, current threat streams, and highlight nationwide aggregated metrics of cross-regional and infrastructure suspicious activity reports.[395]

One of the main concerns identified by the NSI is ensuring privacy protections for those submitting suspicious activity reports. These protections are based on "the protections guaranteed by the First Amendment and limitations on the use of certain factors — including race, ethnicity, national origin, or religious affiliation — in the gathering, collecting, storing, and sharing of personally identifiable information about individuals."[396] The over 70 Fusion Centers abide by the Code of Federal Regulations[397] plus additional peer-to-peer assessments and exchanges to identify shortfalls and gaps in privacy protection implementation.[398]

Information Sharing Programs to Improve National Security

Beyond the critical infrastructure model (discussed separately), there are a variety of programs and offices that were created to increase private-public information sharing, especially regarding information on national security issues, such as weapon proliferation, energy security and international intelligence.

CBP unveiled the Private Sector Intelligence Liaison Office (PSILO) concept in 2012. The concept brings together private sector experts and CBP personnel in an attempt to better identify and address issues of interest to both DHS and private sector industries. According to CBP, the private sector experts are pulled from security, customs compliance and sourcing departments of importers to offer insight and advise CBP on a number of critical issues.[399] These representatives are not collocated with CBP personnel, but rather the two parties interact predominately via phone, email and conference calls.

As of January 2013, CBP had deployed three liaison officers in the semiconductor, pharmaceuticals, and steel trade industries. It indicated plans to deploy two additional officers in the auto and petroleum industries, although the current status is unclear.

The Office of the Director of National Intelligence has had a similar effort to increase partner engagement, including with the private sector, in order to garner important intelligence information and support its analysis.[400] In 2009, for example, its private sector office created a Trade Association Partners Group. Quarterly meetings of trade group representatives and intelligence community officials provided government with insights from a previously under-utilized segment of the private sector while also working to address industry needs for maintaining security. [401]

The FBI has one of the longest-standing private-public partnership associations in InfraGard, with representatives from industry, academia, and state and local law enforcement agencies.[402] InfraGard was originally focused on cyber-crimes but expanded more broadly to critical infrastructure, corralling over 80 local chapters to share information on potential threats to key infrastructure.[403] Membership in this non-profit association is open to all types of businesses as well as research institutions and local law enforcement.[404]

At a more senior level, the FBI founded the Domestic Security Alliance Council in 2003 by inviting senior security executives from large corporations to advise the agency. Modeled on the State Department's Overseas Security Advisory Council, the FBI Council has expanded more recently to include government agency partners, including DHS, State Department and FEMA, and is expanding to FBI regional offices. It is an attempt to better coordinate multiple efforts across government and within the FBI.

Information Sharing Within the Private Sector

Information needs are growing for businesses as well as individuals. For businesses, as the supply chain lengthens, less is known and more knowledge is needed to manage operations successfully. More knowledge on customers, suppliers and the physical and political environments can help inform company policies and processes to increase returns and reduce risk. Whether it is identifying trusted business partners that can provide timely, quality supplies or ensuring that products are not employed for unauthorized end uses, companies forge relationships based on expectations of performance. Even individual consumers are no longer restricted to buying goods from the shop on the corner or using the only local electrician to service our homes — but they need information to make judgments on quality and reliability.

To meet new needs, various third-party commercial and non-profit efforts have sprung up to develop and share information. For instance, Better Business Bureau ratings long have been a

way to judge the services provided by business, and now even by charities. Similarly, Consumer Reports has provided product information and ratings for decades. More recently, by crowdsourcing and vetting information, Angie's List developed a way for consumers to inform themselves on contractors and other service providers. Those wanting to make a contribution or to invest their money can look also to Charity Navigator, Morningstar, and various ratings of socially-responsible funds. The Insurance Institute for Highway Safety provides vehicle safety rating information, and US News & World Report gives college ratings. These ratings may not be without controversy.

On the commercial side, the need for merchants to gain information on the credit-worthiness of buyers was the genesis of credit-rating agencies like Experian. That company dates its origins to the early 1800s and London merchants sharing information on defaulters.[405] Commercial rating systems have sprung up in other areas, too. Oil field operators need to know the speed, quality and safety of their suppliers/contractors. Insurers need to know the quality of the home or office building they are insuring against natural hazards. And shippers, LSPs and insurers need to know the quality of the ships they use.

Private firms such as RightShip have been founded to meet the need for more information on ocean vessels. RightShip provides a "ship vetting information system" that takes publicly available information as well as information garnered from confidential sources to evaluate risk factors associated with a cargo ship embarking on a specific passage. Star ratings of one to five are given to large, commercial ships.[406] Its rating system was coming into such demand that it was being used (wrongly) as a standard clause in shipping contracts.[407]

Similarly, exporters need to reassure themselves and governments that they are in compliance with US and foreign laws and regulations. Indeed all manufacturers need to make sure they are not violating export and sanctions controls through deemed exports, e.g., the sharing of information or technology with foreign nationals. To help with this, private companies have developed up-to-date, consolidated lists of sanctions regimes, including lists of parties with whom companies cannot deal. Among these blacklisted entities, for example, are "specially designated nationals" (SDNs), whose assets are frozen and who are denied market access privileges. Other companies offer automated compliance checks as well as training programs to help institutionalize good compliance practices in a company.[408]

Dun & Bradstreet is developing regulatory compliance products that could, in the project team's assessment, be adapted to support end-user checks.[409] Of course, critics have questioned the ability of firms such as Moody's, Standard & Poor's and Fitch to give independent, accurate ratings, often citing high marks given to the mortgage-backed securities that helped precipitate the 2008 financial crisis.[410] However, part of the problem in that case was a perverse incentive structure; securities issuers were paying the rating agencies to sustain the ratings assessment process. In short, rating agencies do not provide a foolproof solution, but a transparent end-user rating system similar to that developed for credit markets could help.

There are clear reasons for independent third parties to develop, anonymize and share information. One is the concern shared by many companies of competitive damage that can be wrought from improper sharing of customer information or trade secrets. Another is fear of anti-trust violations. Companies and trade associations must follow strict guidelines when sharing information to avoid government investigation or penalties.[411]

There are notable cases where these strictures are partially relaxed. For instance, as discussed in the next section, greater public-private information sharing is allowed in certain areas related to critical infrastructure. Also, in April 2014, the Department of Justice and Federal Trade Commission affirmed that private companies generally would not come under anti-trust scrutiny when sharing certain kinds of cybersecurity information with one another.[412]

THE CRITICAL INFRASTRUCTURE SECURITY MODEL

Looking in-depth at the critical infrastructure model, particularly as it relates to stakeholder engagement and information sharing, illuminates both challenges and opportunities that apply more broadly, including in the area of export controls and sanctions enforcement.

HISTORY OF CRITICAL INFRASTRUCTURE PROTECTION

Regrettably, meaningful progress often comes only on the heels of major adversity. The 1995 Murrah Federal Building bombing was a wakeup call for the nation — and for Washington. One hundred sixty-nine people lost their lives in that act of domestic terrorism and many more were injured, including small children in the building's daycare center. The blast from the explosive-filled Ryder truck damaged a 48-block area of Oklahoma City. The effects of the losses were felt across government agencies as well as the private sector. How could the nation better protect itself?[413]

Partly as a result of that bombing, government took a closer look at its critical infrastructure. In July 1996, President Clinton issued Executive Order 13010, which acknowledged "certain national infrastructures are so vital that their incapacity or destruction would have debilitating impact[s] on the defense or economic security of the United States."[414] This executive order established the President's Commission on Critical Infrastructure Protection and helped shift the focus of discussion on threats to the nation's security to one that addressed the strengths and weaknesses of the nation's infrastructure. Furthering this focus, in 1998, President Clinton issued Presidential Policy Directive 63 (PPD-63), tasking government and the private sector to develop a plan to reduce critical infrastructure vulnerabilities.[415] The National Infrastructure Protection Plan (NIPP) represents the further development of that partnership.

The NIPP was developed to support integration of various critical infrastructure protection measures into a uniform national effort, as outlined in Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7). This effort requires engaging private sector owners and operators of the nation's critical infrastructure — in collaboration with other actors such as state, local and tribal governments, regional coalitions, international entities and NGOs — to enhance the security and resilience of the nation's critical infrastructure.

Responding to 2013 Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, DHS worked with stakeholders to produce the latest update to the NIPP. The presidential directive defined 16 sectors that perform essential services and comprise the nation's critical infrastructure, consolidating the 18 identified previously in HSPD-7.

As part of the update, the 2013 NIPP highlights security and resilience of critical infrastructure as a central goal of nationwide efforts. The 2013 update incorporates aspects of the National Preparedness System to better align with the National Preparedness Goal as well. The overall intent of the 2013 plan is to help steer a national risk management effort for the nation's critical infrastructure by incorporating the efforts of multiple stakeholders to "strengthen the security and resilience…managing physical and cyber risks through the collaborative and integrated efforts."[416]

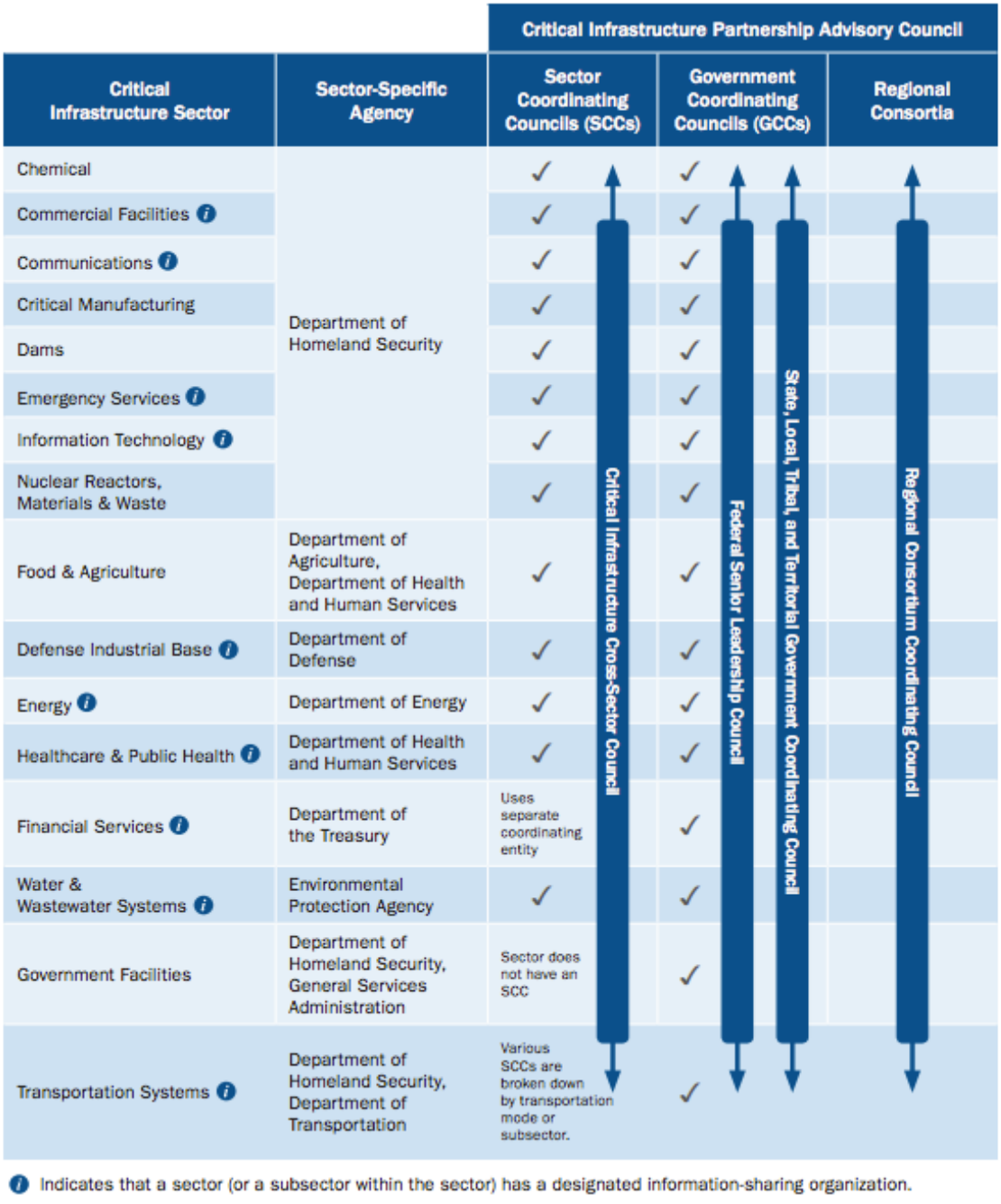
CRITICAL INFRASTRUCTURE ENGAGEMENT AND SHARING

The plan outlines five primary goals, one of which advocates for sharing "actionable and relevant information" on possible threats, vulnerabilities, and other risks to critical infrastructure security and resilience. Noted mechanisms for achieving efficient and effective information sharing include constructing and promoting a common culture of "need to share" across all respective levels and sectors of the critical infrastructure community and utilizing state and local fusion centers.[417] The plan notes that government can help facilitate information sharing by providing pertinent unclassified information from otherwise classified or restricted unclassified reports to private sector partners. Noted industry benefits are detailed as including greater access to actionable information, greater understanding of the risk landscape, and a greater capacity to help government make more-informed decisions pertaining to critical infrastructure security and resiliency.[418]

The success of the information-sharing efforts described in the NIPP depends on active participation in voluntary programs by both government and private sector actors. The structure of the NIPP efforts is founded on a model for public-private interaction and partnership. The partnerships are organized around sector and cross-sector councils — illustrated in the figure below.

The Critical Infrastructure Partnership Advisory Council (CIPAC) was established by the Secretary of Homeland Security to assist with NIPP implementation by enabling interactions among the industry representatives and federal, state, local, territorial and tribal governments. Within the CIPAC structure, government and industry stakeholders may, among other actions, share information on threats, vulnerabilities, best practices, and lessons learned that might then be used to influence policy.[419] The CIPAC provides certain levels of protection for various exchanges, including exemptions from the Federal Advisory Committee Act — thereby allowing members to communicate on threats to the nation's critical infrastructure without discussions being publicly disclosed.[420]

Sector and Cross-Sector Coordinating Structures



		Critical Infrastructure Partnership Advisory Council		
Critical Infrastructure Sector	**Sector-Specific Agency**	**Sector Coordinating Councils (SCCs)**	**Government Coordinating Councils (GCCs)**	**Regional Consortia**
Chemical	Department of Homeland Security	✓	✓	
Commercial Facilities ⓘ		✓	✓	
Communications ⓘ		✓	✓	
Critical Manufacturing		✓	✓	
Dams		✓	✓	
Emergency Services ⓘ		✓	✓	
Information Technology ⓘ		✓	✓	
Nuclear Reactors, Materials & Waste		✓	✓	
Food & Agriculture	Department of Agriculture, Department of Health and Human Services	✓	✓	
Defense Industrial Base ⓘ	Department of Defense	✓	✓	
Energy ⓘ	Department of Energy	✓	✓	
Healthcare & Public Health ⓘ	Department of Health and Human Services	✓	✓	
Financial Services ⓘ	Department of the Treasury	Uses separate coordinating entity	✓	
Water & Wastewater Systems ⓘ	Environmental Protection Agency	✓	✓	
Government Facilities	Department of Homeland Security, General Services Administration	Sector does not have an SCC	✓	
Transportation Systems ⓘ	Department of Homeland Security, Department of Transportation	Various SCCs are broken down by transportation mode or subsector.	✓	

Critical Infrastructure Cross-Sector Council

Federal Senior Leadership Council

State, Local, Tribal, and Territorial Government Coordinating Council

Regional Consortium Coordinating Council

ⓘ Indicates that a sector (or a subsector within the sector) has a designated information-sharing organization.

Source: DHS, "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience," p. 11

As part of CIPAC's overall structure, private sector collaboration is organized into sector coordinating councils (SCCs), comprised of owners and operators of critical infrastructure and

representative trade organizations. SCCs then serve as the primary points of communication of industry to the US government for policy inputs and discussions, among various other activities. The chairs and vice chairs of these SCCs are further organized into a Critical Infrastructure Cross-Sector Council that works within the private industry community to coordinate and manage cross-sector points of interest and initiatives. Government representatives work within Government Coordinating Councils (GCCs) to enhance "interagency, intergovernmental, and cross-jurisdictional coordination" with various government agencies. These councils also work with SCCs on public-private security and resilience efforts.[421]

RESOLVING INFORMATION-SHARING ISSUES

To better enable voluntary disclosures of threat and vulnerability information by industry, the Protected Critical Infrastructure Information (PCII) Program was established under authorities of the Critical Infrastructure Information Act of 2002.[422] Under the program, threat information voluntarily submitted to DHS by critical infrastructure owners and operators can be used in accordance with restrictions spelled out in the 2002 law.

For example, only government employees and contractors who are trained and authorized to use PCII may handle the information submitted. The information is also exempt from Freedom of Information Act requests; state, tribal and local disclosure laws; use in regulatory actions; and use in civil litigation.[423] Owners and operators may submit information physically, electronically or orally — provided that a written statement follows. DHS does not believe the private sector incurs great costs in submitting critical infrastructure information through the program. [424]

To help government share information in return with the private sector, in December 2009, President Obama released Executive Order 13526 which outlines standards for classifying national security information. As a component of the safeguarding measures described in the document, the order states that classified information may be shared with other US agencies or entities, to include private organizations that are part of the nation's critical infrastructure, without consent from the entity of which the information originated. [425] That is, private sector critical infrastructure entities may receive classified national security information provided that they have been granted "a favorable determination of eligibility for access by a [government] agency head, have signed an approved nondisclosure agreement, and have a need-to-know status."[426]

In terms of type of information shared, the types can cause confusion and result in mistakes or the release of protected information. There are a plethora of designations for information categorization, especially "sensitive but unclassified" information, including "sensitive security information (SSI)," "for official use only (FOUO)" and "law enforcement sensitive (LES)."[427] While the unauthorized release of FOUO or LES information will not result in a civil penalty, the unauthorized release of SSI will. SSI is specifically for data related to transportation, however, within SSI there are sixteen categories — creating more confusion on information designation.[428]

In order to facilitate exchange of this information, it is necessary to ensure that the various types of information are applied in a clear and correct manner. Thus, there is a recognized need to facilitate standardization and ensure that the definitions are used harmoniously within the

government and between government and private industry. A White House-led effort to harmonize controlled but unclassified information was started in 2010 but has had unclear results.[429]

The National Infrastructure Advisory Council (NIAC) undertook a major effort to determine "whether the right people are receiving the right intelligence information at the right time to support robust protection and resilience of the Nation's critical infrastructure."[430] In issuing its conclusions in 2012, the NIAC cited substantial improvements in interagency information-sharing processes but

these gains have not been seen in public-private information sharing between the government and the private owners and operators of the nation's critical infrastructure.[431] The Council provided analysis and recommendations to enhance a more bi-directional information-sharing program between the stakeholders of critical infrastructure security and resilience.

The report states that there is a substantive lack of implemented processes to leverage the knowledge and analysis capabilities that are unique to the private sector and a subsequent lack of prioritization. Not only does the private sector not receive the predictive intelligence information, but also the methods by which it does receive information may result in large quantities of late, redundant or potentially conflicting information. As the report details, Homeland Security Information Network-Critical Sectors (HSIN-CS) is only modestly useful "at best" in meeting the needs of the private sector for information.[432]

In order to address these issues, the Council recommended that the government improve information sharing in both content and delivery. The report highlights that DHS may improve information content by leveraging the wide array of capabilities provided by various partners.[433] This could include seeking commercially available tools for predictive intelligence, for example. A recommendation for enhanced information delivery centers on ODNI and DHS establishing new dissemination product formats to allow for the creation of information products for owners and operators.[434] The Council also recommends that national fusion centers create a process for sharing information with owners and operators.

The United States Government responded to these recommendations by developing a national strategy for information sharing and safeguarding. Other responsive actions to the report included the formation of a joint initiative among DHS, PM-ISE and ODNI to improve private sector integration into the current ISE processes. [435] As noted in earlier sections, this is an ongoing challenge.

HSINs, ISACs and What's Next?

Information Sharing and Analysis Centers (ISACs) have also become key outlets for information exchange among some industry partners. Where they are active, ISACs serve as "clearinghouses" for certain information thereby allowing it to be anonymized before being shared among members, particularly in the cyber sector. As opposed to the DHS-centric HSIN system, the ISACs are non-profit, member-driven organizations, often with fees for participation at different levels of membership. Established by critical infrastructure owners, these centers are tasked with providing industries "accurate, actionable, and relevant information," however the results are sometimes mixed. ISACs were first formed following release of PDD-63 in 1998, gaining further momentum with release of HSPD-7 in 2003.

The Department of Homeland Security and the US government have attempted to build and expand upon these trusted networks in order to facilitate information sharing so as to reduce industry's vulnerability to numerous threats and increase resilience. DHS has supported sector-specific Homeland Security Information-Sharing Networks (HSINs) in order to share information, including Sensitive But Unclassified information, with partners. In some cases, HSINs as well as ISACs include international partners.

The more nimble, industry-organized ISACs no doubt will continue to expand as threats increase. Following its massive data breach, Target recently joined the Financial Services-ISAC (FS-ISAC) and qualified for participation because it has finance operations. The National Retail Federation, a major trade association, also has announced it is establishing a retailers' ISAC in consultation with the FS-ISAC to help retailers manage cyber risks.

Other trade associations with specific information-sharing needs could do the same.

Pointedly, the new 2013 NIPP calls for:

- A review of what is hindering effective information sharing today, including legal concerns
- An analysis of gaps and overlaps within and across the federal government itself on information-sharing programs, with a view to developing joint doctrine within government as well as standard operating procedures for engagement
- A functional requirements analysis of what each sector needs and the development of data and interoperability standards to facilitate fast, efficient information flows.[436]

These efforts will be critical to improving information-sharing efforts beyond the critical infrastructure sectors. They also could be leveraged to address cross-sector and other national security concerns. Indeed, one of the next steps in improving the federally mandated Cybersecurity Framework is a more focused assessment of supply chain security issues.[437]

CI-Focused Information Sharing Initiatives

Three specific initiatives that focus on critical infrastructure are highlighted below. The cyber threat example shows that a cross-sector approach is possible but needs industry to really drive it to effectiveness. The chemicals sector initiative shows that legislation has been used to protect additional sources of security information that government developed as part of its regulatory

program — and how complex controls and information can be. Finally, the maritime information sharing platform is a look at a specific data-sharing initiative.

Cyber Threats and Information Sharing

The Enhanced Cybersecurity Services (ECS) initiative is a voluntary information-sharing program that helps owners and operators of critical infrastructure improve the protection of their technological systems and facilities by providing classified information on potential or real threats. The program works to enhance an organization's existing cybersecurity capabilities by providing threat indicators to qualified Commercial Service Providers (CSPs). The CSPs are then able to provide better protection to their customers — that is, to critical infrastructure organizations. Such entities include companies like AT&T and CenturyLink, which are both CSPs approved to provide ECS services to their critical infrastructure customers.

As noted by ECS, threat information detected by CSPs is not shared directly between their critical infrastructure customers and the federal government, and therefore the ECS program does not act as a government monitoring system. A critical infrastructure customer of a CSP may wish to voluntarily provide information to the government, in which case the entity may share limited and even anonymized information with ECS. Entities that express interest in participating in the program must be validated through DHS, which uses two main criteria to evaluate candidates — an entity must be US critical infrastructure, or a US NGO.

DHS initially had limited success convincing organizations to take part in the ECS program. While many corporations expressed interest, businesses debated whether the benefits of the program outweigh the costs of implementing the necessary network upgrades for handling the classified information. Reports note that DHS has not been able to efficiently process the approvals for those that have applied to take part.

The DHS Cyber Information Sharing and Collaboration Program (CISCP) launched in 2011 to focus on infrastructure cybersecurity. Companies can share threat and other data with DHS under Protected Critical Infrastructure Information (PCII) rules which protect that data from disclosure. DHS then uses that information to share information back out with industry. DHS has undertaken a pilot program to directly automate cyber-threat data-sharing with the financial services industry. The DHS National Cybersecurity and Communications Integration Center (NCCIC) also oversees the Computer Emergency Readiness Team (US-CERT), which receives and posts threat and vulnerability information to all concerned about cybersecurity.

The Chemical-terrorism Vulnerability Information (CVI) Regime

Within critical infrastructure, there are a variety of sector-specific information- sharing programs, For example, Public Law 109-295 authorized the Chemical-terrorism Vulnerability Information (CVI) regime in 2006 as part of a concerted effort to protect sensitive but unclassified information developed under the Chemical Facility Anti-Terrorism Standards (CFATS) regulation. The intent of CVI is to safeguard information about the nation's high-risk chemical facilities from harmful public disclosures.

A wide range of information falls under CVI designation. Such information includes chemical facilities security vulnerability assessments, site security plans, alternative security programs, and any documents relating to audits or inspections, among others. Only authorized users may possess and/or receive CVI. A chemical facility may disclose CVI to any of its members, provided those members are CVI-authorized and have a need to know. A facility also may choose to share CVI with the private sector or third parties that may be affiliated with the facility, with the same provisos.

A party's need to know status is assessed on a case-by-case basis that also includes an assessment of any and all documents involved. Private sector entities and third parties may become CVI authorized users by completing authorized user training, in which case DHS reviews all information provided and then notifies entities if they are approved.

The difference between Protected Critical Infrastructure Information (PCII) and CVI is primarily how the information is developed. Generally, PCII is submitted by industry and CVI is developed from assessments done to comply with DHS regulations.

Maritime Information Sharing

The National Maritime Domain Awareness Architecture Plan (NMDAAP) is the foundation for the Maritime Information Sharing Environment (MISE), and provides an outline for sharing maritime information among ports, government agencies, public and private organizations, and international actors.

Four architectural views make up the maritime architecture framework, and these views are data, services, security and technical operations. An illustration of the information sharing architecture as described in the NMDAAP is shown below.

Information sharing among participants of MISE is founded on a web-based capability in which data providers and users may share information with common language and a standardized security process. The plan uses NIEM-Maritime as a guide to define its standards. Access to data is controlled by a number of security attributes, thereby limiting the information to indicated agencies, actors, or the greater community — both national and international — as defined.

Only users with trusted systems may share and receive information through the information sharing architecture detailed in the plan. Trusted systems are the IT systems that ultimately allow a user to view and manage all available maritime information.

[318] Mongelluzzo, Bill. "Terminal Velocity." *Journal of Commerce* (July 22, 2013): 15. Accessed January 31, 2014. http://www.apmterminals.com/uploadedFiles/corporate/Media_Center/In_The_News/APM%20Terminals%20Terminal%20Velocity%20article.pdf.

[319] Ibid., 15.

[320] Port of Long Beach. "Middle Harbor." Projects. About Us. Accessed January 31, 2013. http://www.polb.com/about/projects/middleharbor.asp.

[321] Mongelluzzo, Bill. "Evolution of the Smart Port." Key Findings on Terminal Productivity Performance Across Ports, Countries and Regions Journal of Commerce. 2013. Accessed January 30, 2014. http://www.joc.com/port_productivity. 14.

[322] DHS. Science and Technology Directorate. National Center for Risk and Economic Analysis of Terrorism Events (CREATE). *The Impact on the US Economy of Changes in Wait Times at Ports of Entry*. By Roberts, Bryan, Nathaniel Heatwole, Dan Wei, Misak Avetisyan, Oswin Chan, Adam Rose, and Isaac Maya. April 4, 2013. http://create.usc.edu/CBP%20Final%20Report.pdf.

[323] Federal Highway Administration. "Major FHWA Actions (Complete and Pending)." Status of Major FHWA Activities to Implement MAP-21. Presentations. Last modified October 21, 2013. Accessed January 31, 2013. http://www.fhwa.dot.gov/map21/21oct_implementation.cfm.

[324] Svanberg, Johan. "Real-time Container Tracking Is Ready to Take Off." Logistics Arena, June 22, 2013. Accessed December 4, 2013. http://www.logisticsarena.eu/real-time-container-tracking-is-ready-to-take-off/.

[325] Globe Tracker. "Globe Tracker: Smart Container Tracking and it's [*sic*] Impact on Global Ocean Freight." Globe Tracker International A/S. Accessed January 30, 2014. http://www.intermodal-events.com/files/technology_case_study_don_miller.pdf.

[326] For example, see: Marine Traffic. "Live Ships Map." Accessed July 14, 2014. https://marinetraffic.com/en/; Vessel Finder. "Map." Accessed July 14, 2014. www.vesselfinder.com.

[327] SIW Editorial Staff. "Installed Base of Container Tracking Systems Grew 54 Percent in 2012." Security Info Watch, May 20, 2013. Accessed January 30, 2014. http://www.securityinfowatch.com/news/10946261/the-number-of-active-remote-container-tracking-units-deployed-on-intermodal-shipping-containers-was-137000-in-q4-2012-up-from-89000-a-year-earlier.

[328] Svanberg, "Real-time Container Tracking Is Ready to Take Off."

[329] *Container Tracking and Security*. Gothenburg, Sweden: Berg Insight, 2012. Accessed July 14, 2014. http://www.berginsight.com/ReportPDF/ProductSheet/bi-container2-ps.pdf.

[330]SMART Container Chain Management. "A 'Single Window' Platform." Accessed January 30, 2014. http://www.promit-project.net/UploadedFiles/Events/ConferenceIstanbul/Aifadopoulou.pdf.

[331] US National Research Council. Transportation Research Board (TRB). National Cooperative Freight Research Program. *Freight Data Sharing Guidebook.* 2013. Accessed July 14, 2014. http://onlinepubs.trb.org/onlinepubs/ncfrp/ncfrp_rpt_025.pdf.

[332] Ibid., 11.

[333] Ibid., 10.

[334] International Trade Data System (ITDS). *Report to Congress on the International Trade Data System*. Washington, DC: ITDS, December 2013: 1. http://www.itds.gov/linkhandler/itds/news/2013_itds_report.ctt/2013_itds_report.pdf.

[335] Ibid., 8.

[336] Bailey, Douglas. "ITDS-ACE Product Information Committee Progress Report." November 2008. Accessed December 19, 2013. http://www.itds.gov/linkhandler/itds/tsn/product_info_comm/progress_report.ctt/progress_report.pdf.

[337] DHS. CBP. "Importer Security Filing and Additional Carrier Requirements." August 2009. Accessed July 14, 2014. http://www.cbp.gov/sites/default/files/documents/import_sf_carry_3.pdf.

[338] GAO. Supply Chain Security: CBP Has Made Progress in Assisting the Trade Industry in Implementing the New Importer Security Filing Requirements, but Some Challenges Remain. Report no. GAO-10-841. Washington, DC. September 2010: 11. Accessed July 14, 2014. http://www.gao.gov/new.items/d10841.pdf

[339] World Trade Reference. "Advance Manifest Rules for Cargo Information '2-Hour Rule' '24-Hour Rule' Etc." Accessed April 29, 2014. http://www.worldtraderef.com/wtr_site/amr.asp.

[340] DHS. CBP. "Extension of the Air Cargo Advance Screening (ACAS) Pilot Program and Reopening of Application Period for Participation." Federal Register 78, no. 205 (October 2013): 63237-63238. Accessed July 16, 2014. https://www.federalregister.gov/articles/2013/10/23/2013-24856/extension-of-the-air-cargo-advance-screening-acas-pilot-program-and-reopening-of-application-period.

[341] ITDS, *Report to Congress*, 1.

[342] Ibid., 6.

[343] Ibid., iii.

[344] ITDS. Advisory Committee on Commercial Operations. "Automated Commercial Environment (ACE)/International Trade Data System Update." Washington, DC: ITDS, November 13, 2013: 1. http://www.cbp.gov/sites/default/files/documents/05%20C%20%20CBP%201USG_ACE_ITDS_Issue%20Paper.pdf.

[345] Blachere, John. "CPSC ITDS/RAM Pilot System: An IWS Success Story." Presented at the TSN Plenary Session, Washington, DC, September 27, 2013. Accessed July 14, 2014. http://www.cbp.gov/sites/default/files/documents/11_ITDS_CPSC.pdf.

[346] US Food and Drug Administration (FDA). "PREDICT." Import Program. For Industry. Last modified August 24, 2012. Accessed April 14, 2014. http://www.fda.gov/ForIndustry/ImportProgram/ucm172743.htm.

[347] Thompson, John. *Foreign Trade Regulations: Advanced Export Information (AEI) Pilot Program*. Washington, DC: US DOC. Bureau of the Census, January 22, 2014.

[348] ITDS, Report to Congress, iii.

[349] "National Customs Automation Program (NCAP) Test Concerning the Submission of Certain Data Required by the Environmental Protection Agency and the Food Safety and Inspection Service Using the Partner Government Agency Message Set Through the Automated Commercial Environment (ACE)." Federal Register 78, no. 240 (December 13, 2013): 75931-75936. Accessed April 29, 2014. http://www.gpo.gov/fdsys/pkg/FR-2013-12-13/pdf/2013-29724.pdf.

[350] Rowden, Marianne. "Comments on ITDS Product Information Committee's 'Business Case for Using E-Commerce Data to Manage Product Admission at International Borders." Washington, DC: American Association of Exporters and Importers, November 23, 2011: 2.

[351] Executive Order 13659. "Streamlining the Export/Import Process for America's Businesses." *Federal Register* 79, no. 37 (February 19, 2014).

[352] Ibid.

[353] The White House. Office of the Press Secretary. *Fact Sheet: President Obama to Sign Executive Order on Streamlining the Export/Import Process for America's Businesses.* February 19, 2014. Accessed February 19,2014. http://www.whitehouse.gov/the-press-office/2014/02/19/fact-sheet-president-obama-sign-executive-order-streamlining-exportimpor. 1.

[354] "Streamlining the Export/Import Process."

[355] Ibid.

[356] ITDS, Report to Congress, 19.

[357] Author interviews. Fall 2013.

[358] ITDS, Report to Congress, 19.

[359] Executive Order 13629. "Establishing the White House Homeland Security Council." *Code of Federal Regulations*, title 3 (October 26, 2012).

[360] Ibid.

[361] DoS. *Policy Framework and Legal Guidelines for Partnerships*. February 2011. Accessed January 9, 2014. http://www.iecjournal.org/files/state-guidelines-for-partnership.pdf.

[362] White House. National Security Council. Community Partnerships Interagency Policy Committee. *Building Partnerships: A Best Practices Guide*. April 2013. Accessed January 13, 2014. http://www.colorado.feb.gov/useruploads/files/white_house_-_building_partnerships_best_practices.pdf.

[363] Ibid.

[364] US General Services Administration (GSA). "The Federal Advisory Committee Act (FACA) Brochure." Advice and Guidance. Federal Advisory Committee Management. Last modified May 19, 2014. Accessed July 15, 2014. http://www.gsa.gov/portal/content/101010.

[365] DHS. "Homeland Security Advisory Council." Counterterrorism Committees & Working Groups. Organization. About DHS. Accessed July 15, 2014. http://www.dhs.gov/homeland-security-advisory-council-0.

[366] DHS. "Homeland Security Advisory Council Members." Homeland Security Advisory Council. Counterterrorism Committees & Working Groups. Organization. About DHS. Accessed July 15, 2014. http://www.dhs.gov/homeland-security-advisory-council-members.

[367] DHS. *National Infrastructure Advisory Council (NIAC)*. March 4, 2014. Accessed July 15, 2014. http://www.dhs.gov/sites/default/files/publications/niac-brochure-03-04-14.pdf.

[368] DHS. National Protection and Programs Directorate. National Infrastructure Advisory Council. National Infrastructure Advisory Council Charter. November 2013. Accessed July 15, 2014. http://www.dhs.gov/publication/niac-charter.

[369] Author interview with DHS officials. Washington, DC. December 17, 2013.

[370] Ibid.

[371] DHS. Private Sector Office. *Private Sector Resources Catalog*. December 3, 2012. Accessed July 15, 2014. https://www.dhs.gov/sites/default/files/publications/Policy-PSO/private_sector_resource_catalog_December_2012.pdf.

[372] DHS. Federal Emergency Management Agency (FEMA). "Public Private Partnerships." Last updated October 9, 2013. Accessed January 9, 2014. http://www.fema.gov/tools-resources-0.

[374] DHS. Federal Emergency Management Agency (FEMA). *National Preparedness Goal*. September 2011. Accessed December 17, 2013. http://www.fema.gov/pdf/prepared/npg.pdf.

[375] The same report also notes that 90 percent of states and territories consider information sharing a high priority among the core capabilities outlined in the National Planning Frameworks and the National Preparedness Goal. DHS. Federal Emergency Management Agency (FEMA). *National Preparedness Report*. March 2013. Accessed July 15, 2014. http://www.fema.gov/media-library-data/20130726-1916-25045-0015/npr2013_final.pdf.

[376] US Congress. Senate. Committee on Homeland Security and Governmental Affairs. Permanent Subcommittee on Investigations. Federal Support for and Involvement in State and Local Fusion Centers: Majority and Minority Staff Report. 112th Cong., 2nd sess., 2012. http://www.hsgac.senate.gov/download/?id=49139e81-1dd7-4788-a3bb-d6e7d97dde04.

[377] US Department of Housing and Urban Development (HUD). *Hurricane Sandy Task Force Rebuilding Strategy.* August 2013. Accessed July 15, 2014. http://portal.hud.gov/hudportal/documents/huddoc?id=hsrebuildingstrategy.pdf.

[378] DHS. *The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation*. Washington, DC: DHS, December 2011. Accessed July 16, 2014. http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf.

[379] Maritime Security Advisory Committees. 46 US Code § 70112. 2000.

[380] US International Trade Administration (ITA). "Office of Advisory Committees." Accessed May 1, 2014. http://www.trade.gov/oac/.

[381] DHS. Private Sector Office (PSO). *Building Resilience through Public-Private Partnerships Conference — After Action Report*. December 2013. Accessed July 16, 2014. http://www.dhs.gov/event/public-private-partnerships-conference.

[382] The Markle Foundation, a philanthropic organization with a mission of advancing information technology to improve the lives of US citizens, established a task force on national security. Over a number of years, the task force completed several reports on information-sharing processes, policies and technologies to enhance decision-making and national security. These reports have significantly influenced subsequent information-sharing efforts, including the structure and design of the Information Sharing Environment (ISE). See: *Protecting America's Freedom in the Information Age*. New York: The Markle Foundation, October 2002. Accessed July 16, 2014. http://www.markle.org/sites/default/files/nstf_full.pdf.

[383] Author interviews.

[384] White House. *National Strategy on Information Sharing and Safeguarding.* December 2012. Accessed December 18, 2013. http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf.

[385] Ibid., 14.

[386] US Congress. House. Committee on Homeland Security. Majority Staff Report on the National Network of Fusion Centers. 113th Cong., 1st sess., 2013. HR Rep. Accessed December 20, 2013. http://homeland.house.gov/sites/homeland.house.gov/files/documents/CHS%20SLFC%20Report%202013%20FINAL.pdf.

[387] Intelligence Reform and Terrorism Prevention Act of 2004. Public Law 108-458. 108th Cong., 2d sess. December 17, 2004.

[388] The primary users of the Information Sharing Environment include frontline law enforcement, public safety, homeland security, intelligence, defense and diplomatic personnel.

[389] Paul, Kshemendra. "Improving Public-Private Information Sharing in Support of Critical Infrastructure." Presented at the National Infrastructure Advisory Council (NIAC) Quarterly Business Meeting, Washington, DC, November 21, 2013. Accessed July 16, 2014. http://www.dhs.gov/sites/default/files/publications/pm-ise-niac-meeting-2013-11-21-final.pdf.

[390] Information Sharing Environment (ISE) Management Plan. "Introduction." Accessed July 16, 2014. http://info-sharing-environment.github.io/management-plan/.

[391] DHS. "Report Suspicious Activity." Accessed July 16, 2014. http://www.dhs.gov/how-do-i/report-suspicious-activity.

[392] DoJ. Bureau of Justice Assistance. National Criminal Intelligence Resource Center. *Nationwide SAR Initiative: Fact Sheet*. January 2014. Accessed May 9, 2014. http://nsi.ncirc.gov/documents/Nationwide_SAR_Initiative_Fact_Sheet_2014.pdf.

[393] DoJ. Bureau of Justice Assistance. *Suspicious Activity Reporting Training for Hometown Security Partners*. March 2012.

[394] Information Sharing Environment (ISE). "NSI and NMIO to Release SAR Training for Maritime Industry and Ports." ISE Blog. Last modified February 22, 2013. Accessed July 16, 2014. http://www.ise.gov/blog/national-maritime-intelligence-integration-office/nsi-and-nmio-release-sar-training-maritime.

[395] DoJ. Bureau of Justice Assistance. National Criminal Intelligence Resource Center. *Nationwide SAR Initiative: Annual Report 2012.* August 2013. Accessed May 9, 2014. http://nsi.ncirc.gov/documents/NSI_Annual_Report_2012.pdf.

[396] DoJ. Bureau of Justice Assistance. National Criminal Intelligence Resource Center. *Nationwide SAR Initiative: Privacy Fact Sheet*. 2014. http://nsi.ncirc.gov/documents/SAR_Privacy_Fact_Sheet_2014.pdf.

[397] Executive Order 12291. "Criminal Intelligence Systems Operating Policies." *Code of Federal Regulations*, title 28, §23 (1998).

[398] DOJ, Nationwide SAR Initiative Annual Report 2012, 15.

[399] As noted in the concept fact sheet, private sector representatives will offer knowledge on enforcement issues pertaining to developments in intellectual property rights, anti-dumping and countervailing duty, and trade preferences areas.

[400] ODNI. "Partner Engagement." About. Accessed July 16, 2014. http://www.dni.gov/index.php/about/organization/partner-engagement-partnerships

[401] Millis, Linda. Interview by authors. Washington, DC. December 12, 2013.

[402] InfraGard. "Home." Accessed May 1, 2014. https://www.infragard.org/.

[403] US Federal Bureau of Investigation (FBI). "InfraGard: A Partnership that Works." Stories. News. March 8, 2010. Accessed July 16, 2014. http://www.fbi.gov/news/stories/2010/march/infragard_030810.

[404] InfraGard. "Home."

[405] Experian. "History." About Experian. Accessed July 16, 2014. http://www.experianplc.com/about-experian/history.aspx.

[406] Rightship. "SVIS™." Products. Accessed July 16, 2014. http://site.rightship.com/products/svis%E2%84%A2/; Author interviews.

[407] Baltic and International Maritime Council (BIMCO). "Risk Assessment Clause Confronts 'Rightship Approval' Fallacy." News. Last modified November 29, 2013. Accessed July 16, 2014. https://www.bimco.org/news/2013/11/29_risk_assessment_clause.aspx.

[408] For example, see: Proven Logistics Solutions. "Home." Accessed July 16, 2014. http://www.provenlogisticssolutions.com/; exportassure. "Home." Last modified 2014. Accessed July 16, 2014. http://www.exportassure.com/; WorldCompliance. "Global Sanctions List." Database Source Lists. Last modified 2013. Accessed July 16, 2014. http://www.worldcompliance.com/en/compliance-database/global-sanction-list.aspx.

[409] Author interviews with D&B representatives. See also: "D&B Compliance Solutions." Regulatory Compliance. Enterprise Solutions. Business Credit. Accessed July 16, 2014. http://www.dnb.com/business-credit/enterprise-solutions/regulatory-compliance.html.

[410] The Economist. "Credit where credit's due." The Economist, April 19, 2014. Accessed July 16, 2014. http://www.economist.com/news/finance-and-economics/21601020-ratings-industry-has-bounced-back-financial-crisis-credit-where.

[411] Federal Trade Commission (FTC). "Spotlight on Trade Associations." Dealings with Competitors. Guide to Antitrust Laws. Competition Guidance. Tips & Advice. Accessed July 16, 2014. http://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/dealings-competitors/spotlight-trade; Federal Trade Commission and DOJDoJ.. *Antitrust Guidelines for Collaborations Among Competitors.* April 2000. Accessed July 16, 2014. http://www.ftc.gov/sites/default/files/documents/public_events/joint-venture-hearings-antitrust-guidelines-collaboration-among-competitors/ftcdojguidelines-2.pdf.

[412] Federal Trade Commission (FTC). "FTC, DOJ Issue Antitrust Policy Statement on Sharing Cybersecurity Information." Press Releases. News & Events. April 10, 2014. Accessed July 16, 2014. http://www.ftc.gov/news-events/press-releases/2014/04/ftc-doj-issue-antitrust-policy-statement-sharing-cybersecurity.

[413] GAO. *Combatting Terrorism: FEMA Continues to Make Progress in Coordinating Preparedness and Response*. March 2001. Accessed December 21, 2013. http://www.gao.gov/assets/240/231168.pdf; Brown, Kathi Ann. *Critical Path: A Brief History of Critical Infrastructure Protection in the United States*. Fairfax, VA: Spectrum Publishing Group, Inc., 2006. Accessed January 28, 2014. http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/07/CIPHS_CriticalPath.pdf.

[414] Executive Order 13010. "Critical Infrastructure Protection." *Code of Federal Regulations*, title 3 (July 16 1996).

[415] Presidential Decision Directive-63. "Critical Infrastructure Protection." *Federal Register* 63, no. 150 (May 22 1998): 41804.

[416] DHS. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. December 2013. Accessed July 16, 2014. http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience.

[417] Ibid., 23.

[418] Ibid., 17

[419] DHS. *Charter of the Critical Infrastructure Partnership Advisory Council*. March 2012. Accessed January 8, 2014. http://www.dhs.gov/xlibrary/assets/cipac/cipac-signed-charter-2012-3-16.pdf.

[420] Ibid.

[421] DHS. *Critical Infrastructure Partnership Advisory Council Annual Report*. 2013. Accessed January 22, 2014. http://www.dhs.gov/sites/default/files/publications/CIPAC_2013_annual_report.pdf.

[422] Critical Infrastructure Information Act of 2002. 6 US Code §§ 131-134. 2001.

[423] Ibid.

[424] DHS. "Protected Critical Infrastructure Information (PCII) Program." Accessed January 13, 2014. http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program.

[425] Executive Order 13526. "Classified National Security Information." *Code of Federal Regulations*, title 32 (December 29, 2009).

[426] Ibid. The order designates the National Archives Information Security Oversight Office as the overseeing body for implementation of and compliance with the standards presented.

[427] DHS. *Safeguarding Sensitive but Unclassified Information*. May 11, 2004. Accessed July 16, 2014. http://www.fas.org/sgp/othergov/dhs-sbu.html.

[428] DHS. Transportation Security Administration (TSA). Sensitive Security Information Program. "SSI Training for Maritime Stakeholders." Accessed May 1. 2014.

[429] National Archives. "CUI Chronology." CUI. Accessed July 16, 2014. http://www.archives.gov/cui/chronology.html; GAO. *Managing Sensitive Information: Departments of Energy and Defense Policies and Oversight Could Be Improved*. March 14, 2006. Accessed July 16, 2014. http://www.gao.gov/products/GAO-06-369.

[430] DHS. National Infrastructure Advisory Council. *Intelligence Information Sharing: Final Report and Recommendations*. January 2012. Accessed July 16, 2014. http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf.

[431] Ibid.

[432] The NIAC report notes that the HSIN-CS does not meet all of the requisite needs of private sector owners and operators, and that its platform does not fully leverage technological tools that may contribute to more time-sensitive information needs.

[433] US Department of Homeland Security (DHS), *Intelligence Information Sharing*, 34.

[434] Ibid., 48.

[435] ODNI. Program Manager of Information Sharing Environment (PM-ISE). *Information Sharing Environment: Annual Report to the Congress*. June 30, 2013. Accessed January 6, 2014. http://www.ise.gov/sites/default/files/2013_ISE_Annual_Report_Final.pdf.

[436] DHS, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, 23-24.

[437] DOC. National Institute for Standards and Technology (NIST). *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*. February 12, 2014. Accessed July 16, 2014. http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

Modernizing Risk Management

Government and industry alike are recognizing the imperative of cross-functional (and sometimes, cross-sector) collaboration in the fast-paced, interdependent world of global value chains. To achieve more efficient and effective policies and processes, such collaboration requires broad stakeholder engagement and information sharing among trusted parties. The challenge is crossing the threshold where collaboration yields net gains for each constituency.

To achieve those gains, industry and government have to turn data and other information into knowledge and assessments that ultimately inform and affect actions. For the private sector, this means identifying practices that best achieve desired outcomes and by developing ways to codify those practices, including through participation in the development and adoption of clear standards and sometimes the receipt of certain ratings. For government, this means developing better ways to differentiate risks to national security and then institutionalizing incentives for the private sector to help government in this differentiation process.

From its consideration of risk management, the project team found the following:

- Standards have long been important to industry and society as a means to efficiently manage business and government operations and to inform risk management. In an era of global value chains, they are increasingly significant.
- Insurers and others typically seek joint development of information to drive risk assessments after a loss. Collaborative development of risk information and standards for predictive analytics and better risk management is still in its early stages.
- Efforts to standardize trade-related data are gathering momentum with the International Trade Data System implementation.

We begin below with a brief history of standards development and a more detailed look at several standards and best practices global value chains. We then consider how standards may be used in risk pricing and management. We conclude with an overview of the insurance sector and consider both its current and potential contributions to national security

PRIVATE SECTOR STANDARDIZATION

Historically, standards developed to ease communication, to enable interoperability, and to provide safety assurances to users/customers. Industry has been at the forefront of standards development as it sees the need for voluntary systematization of products and processes.[438] But government has also sometimes spurred standards development.

In terms of safety, standards often develop after a tragic event. Fire-equipment standards arose after a tragic Baltimore fire in 1904, when surrounding cities' fire departments found their hoses did not fit Baltimore hydrants.[439] Today, global garment worker standards are being scrutinized after a Bangladeshi garment factory collapsed killing over 1000 workers; socially-responsible/safety-conscious customers as well as corporate liability concerns are driving the movement.

Organizations to establish these standards also come out of tragedies, with norms, best practices and then standards being developed among smaller groups and then spreading. After the 1971 Three Mile Island nuclear plant accident, the US nuclear industry, upon the recommendation of a federal commission, formed and funded the Institute of Nuclear Power Operators (INPO) to develop detailed safety standards.[440] INPO performs peer reviews and rates plants, with its rating said to be used by the industry's mutual insurer. The 1986 Chernobyl nuclear disaster led to the formation of the World Association of Nuclear Operators, sharing safety standards and peer reviews internationally.[441]

Insurance companies have often been the ones who seed fund the development of best practices research that can translate into concomitant standards - and better risk assessments and management. After the 1893 Chicago World's Fair (and concerns about new electrical gadgets), fire insurance underwriters and some electrical equipment manufacturers supported a testing laboratory for William Merrill, an entrepreneur whose work led to the establishment of the Underwriters Laboratories and was the genesis of today's National Fire Protection Association (NFPA) and its standards.[442]

Similarly, in more recent times, having witnessed unprecedented natural-disaster-related losses, the insurance industry funded the Insurance Institute for Business and Home Safety and its large multi-risk research and training facility to test the performance of buildings against hazards from high winds to wildfires and hail.[443] This helps to assess risk and mitigate losses for the insured as well as the underwriters.

Concerns about safety, privacy, humanitarian abuses and ultimately liability have driven standards development. The US government supported the development of standards for private security companies as it increased its use of defense contractors in the field. Today, all private security defense contractors have to adopt the standard, which has been submitted to ISO for adoption as an international standard. The United Kingdom also requires the standard for its private security contracts.[444] The logic is compelling: If you want these government contracts, you have to comply. In addition, the move toward requiring security firms to have liability insurance by countries such as Germany will increase the interest in standards and verification of compliance.[445]

General enterprise performance standards are being widely developed. The International Standards Organization (ISO), with 164 national standards accreditation bodies, has issued nearly 20,000 standards. Developing countries are increasingly looking to ISO certifications to improve their management systems.[446]

The most popular standards are ISO 9000 on quality and ISO 14000 on environmental management systems, with worldwide certificate holders numbering over 1 million and over 250,000 respectively.[447] Large international firms, such as oil companies, are requiring its suppliers and subcontractors to be certified as compliant with these standards even to bid on certain contracts, a private equity investor, a freight forwarder, and a standards developer told Stimson.

The US representative to ISO is the American National Standards Institute (ANSI). It oversees the development of voluntary consensus standards through other US-based specialized bodies it accredits to develop guidelines and standards and complete third-party certifications of standards conformance.[448] Accredited US standards developers include highly specialized groups, such as for the financial services industry, as well as more general ones such as ASIS, which focuses on security. These organizations are accredited by ANSI, but they develop standards among their members and stakeholders internationally. Domestically developed standards often receive international acceptance.

Sometimes standards do not work. Either they do not find wide adoption, or they do not have the desired benefits following adoption. As one example, the Private Sector Preparedness Standard (PS-Prep) developed by DHS is a voluntary private sector preparedness accreditation and certification program which Congress required DHS to develop.[449] The program designated as PS-Prep compliant three existing standards from BSI, ASIS International and the National Fire Protection Association (NFPA).

According to a standards certifier, the PS-Prep certification has been adopted by two companies, and only an office within each company has been certified. Responding to the project team's inquiry on what lessons could be learned from the PS-Prep effort, DHS leadership said that for standards to be effective, the cost-benefit breakdown must be weighted unambiguously toward benefits, and PS-Prep did not have clear benefits.

The lessons to be learned from this are twofold:

- Government may be able to help develop and recognize standards but unless there are clear advantages to businesses in using the standards, they will not be adopted, and
- Historically, the insurance industry has been responding to losses rather than anticipating them and has not looked very systematically at how standards can help reduce losses and limit liability.

However, this is changing. Both government and industry, particularly the insurance industry, acknowledge that more aggressive and collaborative risk management is needed. This owes to a growing recognition that risks are increasingly networked and can have worldwide, systemic effects. It is possible because of the availability of troves of new data and of advanced computational ability and because of the understanding of the benefits of increased collaboration for gaining more data and sharing the burden of the assessments.

PROMOTING TRADE STANDARDS AND BEST PRACTICES

In addition to many government supply chain security initiatives, industry has developed a number of relevant standards.

The International Standards Organization (ISO) is an independent, international organization that has developed technological and manufacturing standards for industry since 1946.[450] It has developed a variety of standards that specify requirements for supply chain security management.[451] The standard ISO 28000 series, for example, is designed to help mitigate risks to people and cargo within the supply chain and address potential security issues at all stages of the value chain.[452] It was developed to harmonize with related ISO standards, such as ISO 9001 (quality management) and ISO 14001 (environmental management).

The ISO 28000 requirements can be applied by organizations regardless of their size and industry sector, and at any stage of the production or supply process. The standard includes provisions to:

- establish, implement, maintain and improve a security management system;
- assure conformity with security management policy;
- demonstrate such conformity;
- seek certification/registration of conformity by an accredited third party organization; or
- make a self-declaration of conformity.[453]

The benefits to companies are numerous. The standards prevent running up costs for multiple certifications, and allowing for the pooling of available transport security standards in one unified management system. This further optimizes company processes and ensures that its supply chain remains free of disruptions. In addition, the company is able to present itself as a professional and responsible partner to customers, authorities, and investors.

The Transported Asset Protection Association sets the standards for the trucking and air cargo companies concerning the protection of high value theft targeted assets (HVTT) during shipping, including (but not exclusively) electronic goods, pharmaceuticals, industry parts, and high-end consumer goods. [454] The TAPA standards are broken down into three overarching areas: freight security requirements (FSR), Trucking Security Requirements (TSR), and Air Cargo Security Standards (TACSS).[455] Each of these areas has its own unique goals and standards, necessitating separate requirements and certification procedures. However, all three involve a review by TAPA-affiliated auditors, and a ranking system that reflects their compliance with the standards. Thus, consumers are aware of the security that is guaranteed when using a TAPA-reviewed transport company.

The certification standards fall under eleven categories: management commitment and support, physical security, personnel security, employee integrity, data and information security, goods and conveyance security (where applicable), closed/secure cargo transport units, additional air cargo security requirements.[456]

ASIS International, an organization for security professionals, has developed a variety of security standards for industry. Past efforts have concentrated on setting private security best

practices and standards. However, currently ASIS is developing standards to improve risk management within the supply chain.[457] The *Resilience in the Supply Chain Standard (SPC.3)* "provides auditable criteria to prevent, prepare for, respond to and recover from a disruptive event using a comprehensive approach to managing risks thereby eliminating the siloing of risks and their impacts."[458] The *Supply Chain Risk Management Standard: A Compilation of Best Practices (SCRM*, co-developed with the Supply Chain Risk Leadership Council, will provide a baseline for best practices to mitigate supply chain risks.[459]

Industry also has taken steps to develop standards for compliance with export controls. Exporters today must comply with an increasingly complex array of controls, imposed by multiple governments and international organizations, to address many different security and policy objectives. At the company level, this regulatory burden has increased compliance costs and elevated compliance risk. Moreover, exporters vary greatly in size, organization, operational practices, and maturity, and these differences often compound the toll brought by regulatory changes.

Private sector standards include efforts by broader industry groups, including the Coalition for Excellence in Export Compliance (CEEC), which brings together exporter representatives from a variety of sectors in order to create a set of standards for the major areas of export control, and ensure a market-savvy security policy. The group notes that there is no perfect set of export compliance procedures, but a more unified set will have benefits for both the government and the export industries.[460] CEEC has outlined eight areas of standards to ensure legal compliance.

Despite the fact that there is no international consensus on the import/export process, there is also an effort by the intergovernmental organization community to increase predictability, transparency and overall security within the international supply chain.

In December 2013, member countries of the World Trade Organization (WTO) concluded a significant agreement on trade facilitation measures as part of the "Bali Package." The accord aims to promote equity and transparency across the customs processes of WTO member states to increase efficiency, and thus economic benefits, for all members.[461] It stipulates a minimal standard for government accountability in changes to trade laws, allowing private industry in member states to comment on proposed legal and regulatory changes to export/import regimes.[462]

Regarding transshipments, another area of proliferation concern, to ensure proper compliance and mitigation of security risks, various US government and international agencies have offered best practices to better harmonize joint industry and government efforts to mitigate transshipment risks. BIS, for example, released a set of recommendations that be broken into several areas of industry best practices:[463]

- Ensure proper verification and due diligence on end users and LSPs by obtaining certification of credentials, and communicating red-flag users to both industry partners and government through information technology.
- Maintain trusted relationships with third parties, especially in routed transactions, including building relationships with LSPs with proper compliance programs.
- Sustain proper information exchange, including communicating to end users and government information on export control classification and destinations. This includes

providing classification numbers and using AES to speed processing and maintain accuracy.

Similarly, the US State Department released a set of best practices aimed at foreign states and industry to ensure proper transshipment procedures for US exports, including dual-use and nuclear materials:[464]

- Ensure proper interagency regulatory apparatus control of transshipment products, including providing customs and enforcement officers with the proper tools, funding and legal protections to carry out inspections and seize cargo.
- Ensure coordination with international partners, including the exporting and end-use country, as well as with private industry. This includes establishing proper information exchange with counterparts, and adopting internationally endorsed manifest collection requirements.
- Ensure industry outreach, including stronger internal compliance, and certify that LSPs understand their obligations for mitigating transshipment and are aware of the associated penalties.

In October 2013, the US Census Bureau released compliance best practices for US and foreign LSPs and exporters. In light of the growing emphasis on efficiency and accuracy of data, the Census Bureau's and other government agencies' best practices are geared toward ensuring the application of AES, which helps to ensure compliance, correct errors and increase efficiency of the entire filing process.[465]

In March 2013, the Census Bureau finalized a new set of reporting requirements for US exporters. The new requirements include mandatory filing of a new data element on "ultimate consignee type"; US exporters must designate the ultimate consignee for each export transaction as one of four types: Direct Consumer, Government Entity, Reseller or Other/Unknown.[466] As explained in the final rule, the Census Bureau added the Other/Unknown option following industry feedback on an earlier draft. While this data element will not highlight much further information about the ultimate consignee — particularly with the addition of the Other/Unknown option — government felt the risk-segmentation benefits continued to warrant the new requirement.

International Data Standardization

Increasing international standardization highlights a larger effort by government and private industry to improve the efficiency and security of export/import processes through utilizing advanced data systems to facilitate data exchange among government and industry partners.

As acquisition of data increases, there is a need for standards regarding the type of information submitted, including product identification numbers. An international non-profit association, GS1, has its origins in an early 1970s effort in the US to develop Universal Product Code (UPC) symbols.[467] GS1 subsequently developed global trade item numbers (GTINs).[468] It is working with the WCO to coordinate on data standards and interchange.[469] With countries relying on international partners to flag suspicious transactions, creating a more uniform system of data

storage would allow for the exchange of information as well as improve efficiency in the customs process by reducing errors resulting from differences in reporting.[470]

The ITDS Board of Directors and the committees it oversees have cited adoption of GTINs as a positive development for both government and industry. Pilot projects employing standardized GTINs reportedly have increased trade efficiency by reducing confusion related to item numbers while enhancing government's ability to verify a product's chain of custody through a cloud-based, track-and-trace system.[471] However, the American Association for Exporters and Importers, an industry association, has voiced concerns that a new data system might not be the appropriate solution. Instead, it says, Congress should assess what data is needed to "shrink the size of the haystack."[472]

In addition to private sector efforts to improve global interoperability of trade data, industry groups may be a key ingredient in developing security standards. In some cases, when adopted by enough of the industry members, these standards have become a prerequisite for doing business in the sector.

For example, the Transported Asset Protection Association (TAPA) sets standards for trucking and air cargo companies for the protection of high-value, theft-targeted assets (HVTT) during shipping. TAPA uses a compliance standard certification program, and companies and insurers are increasingly using TAPA certification as a prerequisite for employment of carriers. The International Air Transportation Association has set similar standards for air carriers through the Secure Freight Program.[473]

Another industry effort, still in its formative stages but worth noting, aims to bring greater visibility to shipping containers in transit. INTTRA, the world's largest provider of automated data services, provides information on the quality of data that shipping companies submit. According to INTRRA, "the delivery of high-quality data is a key element of INTTRA's strategic vision to drive enhanced supply chain shipment visibility in global trade."[474]

RightShip, an Australian company, also has improved carrier transparency with its Ship Vetting Information System, which provides customers with up-to-date information on maritime vessels, including potential risks of use.[475] Both INTTRA and RightShip aim to improve overall maritime shipping security by setting and "enforcing" standards through a transparent, data-driven vetting process.

USING STANDARDS FOR PRICING AND RISK MANAGEMENT

To what extent can standards compliance be used in the marketplace as an indicator of risk? In terms of insurance policies, the answer seems to be, "not quite yet, but maybe soon." For investors, meanwhile, compliance matters, but supply chain security and export compliance is but one aspect of corporate risk.

IN INSURANCE

As pointed out in *Insurance & Behavioral Economics*:

> "[I]nsurance executives often appear to misunderstand their own product in part because of uncertainty: they cannot predict catastrophic weather events, health care cost inflation, or the amount of interest they will earn on their reserves. Paradoxically, managers in the business of bearing other peoples' risks often appear to think (or hope) that they can avoid most of these risks....The industry has made astounding mistakes in the past from which it has learned the hard way….It was only after Hurricane Andrew, when nine property insurers became insolvent, that there was a recognition that companies would have to charge much higher premiums to protect coastal properties against hurricanes."[476]

After these and other significant natural disaster losses, the Insurance Institute for Business & Home Safety funded research into building and business resilience that has led to its FORTIFIED™ program certification and the establishment of trained third-party evaluators. Based on this work, the Department of Homeland Security announced in November 2013 a DHS Resilience STAR™ Home Pilot Project as a government-led, public-private initiative: "Through the pilot project, DHS will work together with the private sector to engage homeowners, builders and contractors in communities at high risk for certain natural disasters to identify proactive steps to enhance the resilience of the homes."[477]

Working with the insurance industry to support such a standards-based program came from the Hurricane Sandy Rebuilding Task Force, which noted no certification programs to promote building resilience similar to ENERGY STAR and the Leadership in Energy and Environmental Design (LEED) program developed by the US Green Building Council.[478] The actual project will involve some retrofitting or new construction.

DHS says it wants to think more broadly about resilience incentives and that while insurance has played a key part, other incentives have been important, too. For example, Alabama has in its tax code up to $3,000 in tax credits for retrofitting properties. IBHS retrofitting generally costs between $400 and $1,100 to make a home five times more capable of withstanding wind. Zoning waivers may also be possible. In exchange for standards compliance, such waivers may allow a developer to build by a river, or allow local communities to get better bond ratings if they have more properties that have a Resilience STAR.[479]

It will be some time before the Resilience STAR rating concept is applied to aspects of the supply chain, but that is a goal of the DHS office overseeing the program. The chain is complex and niche markets in the industry where this will be an advantage are yet to be identified.[480]

It is one thing to define the best practice or standard that can achieve the benefit of reduced risk, it is another to prove that the standard is being applied. A key question is: has a reliable, independent third party verified standard compliance?

When a company that signed up for a standard does not adhere to that standard, the utility of the standard is diminished for everyone involved. The chemical industry's Responsible Care initiative[481] was criticized for being a public relations tool used to avoid industry regulation after a Responsible Care company, Draslovka Kolin, was fined in the poisoning of the Elbe with cyanide.[482] Environmental activists also question the true value of the voluntary initiative.[483] The Responsible Care Global Charter was being updated in 2013.

Standards have varying levels of recognized compliance. They range from self-evaluation and attestation to certification to accreditation. Certification requires a third party to attest to a

company's standards conformity. Accreditation applies to third parties performing the certification service.[484] A standard now exists for certification bodies to implement standards for themselves: ISO/IEC 17021:2011, *Conformity assessment: Requirements for bodies providing audit and certification management systems.*[485]

Not all companies that are compliant with ISO management system standards find the need to be independently certified. Their internal auditors may be even better at ensuring standards compliance than an external auditor who is not as familiar with the company, according to a standards developer.[486]

Given the complexity, thus far, the direct relationship between an insured's compliance with certain standards and underwriters' risk pricing of products to the insured do not appear to have been well correlated. The supply chain standards that have been promulgated thus far such as C-TPAT have not obtained explicit insurance benefits, although compliance with certain standards is used as a broad risk indicator. Insurance industry representatives have stated to the Stimson Center that perhaps they have not fully grasped the liability implications of certain standards adherence or non-adherence.

Assessing the standards against which insured losses can be calculated is still a new area (further discussed in the insurance case study). The already-mentioned ship-vetting company RightShip works with insurers such as Lloyds to help assess the risks of ship transport. By vetting specific "ships and transport and evaluating the potential risks such as the ship's structural integrity, competence of owners, managers and crew, past casualties and incidents," the company helps to evaluate the risks associated with a particular charter. This in terms helps underwriters to price policies. The fact that a private company like this has sprung up shows the movement among insurers as well as those contracting vessels to better understand risks. RightShip is now working with IBM to refine its predictive analytics.[487]

Even when insurance companies do not help directly drive the standard development or the rating company work as they have with the building resilience standard and the ship charter ratings, insurance companies certainly consider some standards as an indicator of risk. Insurers have looked to the private security guard standard for vessels and considered how private security guards onboard a vessel both decrease piracy risks but also may increase other risks, such as when a guard acts mistakenly against a fisherman. Germany is one country looking to requiring ships to have liability insurance to cover the latter event.[488]

Predictive Risk?

"We're not there yet! And whoever figures it all out will get very rich."

Insurance executive
(author interview)

For Companies and Their Lenders and Investors

Insurance — with its cost, terms and general availability — is but one area where companies have been motivated to consider their standards adherence and risk management practices. Standards, best practices, and risk management all come into play as companies move toward better enterprise-wide risk management and increasingly identify and value the risks across their business operations. By adopting standards or following best practices, companies indicate

publicly that they operate by these standards. The public benefits can be product/service differentiation: to the customer (sometimes a requirement in government and private contracting situations), to the investor, to the employees or general public, to company service providers such as banks and the afore-mentioned insurers as well as to government (for regulators and program managers).

This move toward a broader company understanding of standards' value-add and risks is supported by different organizations and being increasingly required by regulators. ISO is publishing in 2014 a new international standard on asset management systems to help companies identify, value and manage the integration of their tangible and intangible assets, including reputation.[489] The already developed ISO 31000 series provides companies with guidance on risk management.[490] The Internal Control-Integrated Framework published in 1992 by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) has been updated to help companies comply with Sarbanes-Oxley Act (SOX) Section 404 requirements.[491]

Risk ratings for companies are important to both lenders and equity investors.

The Securities and Exchange Commission (SEC) has a role to play in considering company compliance with standards and its overall risks — which in turn affect ratings. Its disclosure requirements related to company risks have expanded over the years. SEC staff has recommended that all disclosure requirements in prospectuses be reviewed.[492] SEC Chair Mary Jo White noted that expanded risk disclosures in company filings has also come about due to "company's decision to take a defensive posture and disclose more information rather than less to reduce the risk of litigation claims that there was insufficient disclosure."[493] The risk disclosures vary by company but include climate change risks, terrorism risk exposures, and other material risks.

However, unless a company loses its export privileges or gets debarred from government contracting, the financial penalties have been generally easy for companies to absorb. The effect on the company for non-compliance with exports and sanctions tends to be more individual specific, with someone losing his/her job; and the fears of jail time are the especially-keen drivers of compliance according to company officials and their lawyers. These individual costs and the corporate effort of having to continue to spend time on auditing and fixing compliance programs and employing outside counsel and being audited are the true costs.[494]

Nonetheless, the reputational losses of regulatory non-compliance are not to be totally ignored. In terms of compliance risks, disclosures related to foreign corrupt practices have very much caught public attention, whereas export compliance and sanctions are less discussed and noted.[495] One reason for this could be that general corruption is a larger overall issue in dealings in international business and will often involve big-name companies. Or it could be that no third party is doing the name-and-blame that happens with bribery and bidding scandals and similar corrupt practices.

Public and insider reporting of national security-related suspicious activities can play an important role in uncovering illicit activities. ICE Homeland Security Investigations receives thousands of tips that have led to the shutdown of a human smuggling ring, the arrest of a violent Mexican gang member, and addressed drug smuggling and money laundering.[496]

Engaging the Public's (and Employees') Help?

Might more tips be generated on export and sanctions compliance with a program like the Dodd-Frank Whistleblower Awards? In its first 18 months of operation, that Awards program generated over 3,000 tips and has paid out awards to six whistleblowers. One of these whistleblowers received $14 million for information on securities law violations leading the SEC to recover "substantial investor funds."

With companies under rising pressure to identify, manage and disclose risks, they are likewise compelled to better understand enterprise-wide value drivers. They also must understand the value added not just from their own enterprises but also from the whole value chain they create and are part of as part of a global value chain in their trade — as well as the inherent risks in potential disruptions to that chain.[497]

The way they understand this will change as companies become more sophisticated, including. As a report from the Economist Intelligence Unit concludes, "Increasingly sophisticated data-driven techniques will make risk management more efficient, freeing managers and executives to focus more on the task of aligning risk across the enterprise."[498]

That is, to the extent risks can be somewhat accurately predicted.

For Government

Perhaps the biggest beneficiary of standards setting and compliance measures is government. In short, being better able to identify what commercial variables affect risk allows government to better target scarce resources.

The Insurance Industry: Partnering In National Security

Overview

To date, the insurance and reinsurance space has not been considered extensively in nonproliferation and trade research. Yet insurers and reinsurers are — like financiers — critical facilitators of commerce, including illicit trade.

The insurance industry's risk management toolkit is in a state of modernization. The use of "big data" and predictive analytics is slowly becoming more common in commercial insurance, which lags consumer insurance in this regard. New information sources, new insights, and new standards are all being sought to help devise better models for risk assessment. Brand new risks, such as cyber incidents, as well as evolved challenges from age-old threats, such as piracy, have brought renewed focus to the national security aspects of insurance. The public-private partnership on issues such as flood risks has been reshaped over the last decade in new areas such as terrorism risks. An opportunity exists for government and the insurance industry to engage even more closely to the benefit of national security and the private sector.

As a result of an in-depth look at the insurance industry as it relates to trade and national security, the project team reached these findings:

- While a large and important part of the economy, the insurance industry is poorly understood by those outside the sector. Its relevance to national security is even less appreciated.
- Government can make better use of insurance industry expertise and encourage joint research on risk and resilience. However, government engagement with the sector tends to be fragmented.
- There is potential for new insurance products, including some related to cybersecurity and compliance risk, to advance both national security and industry competitiveness.

INSURANCE BASICS

To examine the intersection of the insurance industry with illicit commerce, terrorism and trade in general, the insurance industry must be considered both for its role as a facilitator of commerce by its helping others to manage risks and as an industry unto itself and a manager of its own risks. In both capacities, the industry plays a role that affects the flow of illicit commerce, but one that has escaped much in-depth study.

Insurance is defined as a "system to make large financial losses more affordable by pooling the risks of many individuals and business entities and transferring them to an insurance company or other large group in return for a premium."[499] Since insurers must set aside monies in anticipation of future payouts that they cannot accurately predict, potential exists for unscrupulous behavior and for heavy price competition. This led to early regulation of the industry. Now a significant industry in the United States and one of the largest industries in the world, the insurance industry is regulated extensively domestically and internationally, not only for consumer protection but also for international financial stability.[500]

The industry is challenged by the multiplicity of regulations in the United States, where each state oversees the insurance market in its state. This has led not only to 50 states and additional territories independently imposing market operating conditions, but also has led to a de facto system of shadow regulators, with attorneys general, governors and other elected representatives weighing in on industry laws, regulations and interpretations.[501]

As a facilitator, the insurance industry helps stakeholders in international commerce create value through risk management. By identifying, pricing and transferring risk, insurance providers help a customer maximize its returns given its particular risk tolerance. The stakeholders in commerce range from manufacturers and technology innovators, to wholesalers, to logistics service providers, to carriers (e.g., air, rail, trucks, ships), to port operators. All these entities, both private and public, make choices on how to manage their risks through self-insurance, captive establishment, and policy coverage and retention levels. In making those decisions, they often consult with insurance brokers and agents.

Insurers must develop relationships with companies to understand their risks and decide how to price risk products for them. However, the insurance provider has its own enterprise risks — from actuarial to operational to financial. The first table below identifies the key actors involved

in providing risk management products to companies. The second table below describes some of the broad categories of risk management products these actors provide.

Key Insurance Industry Actors

Agent	An entity that negotiates an insurance contract on behalf of an insurer as an employee or as an independent agent of the insurer; an independent entity may represent more than one company
Broker	An insurance intermediary who negotiates insurance contracts on behalf of an entity wanting to buy insurance
Captive	An insurance company established to insure the risks of its owners and used in place of or typically in addition to commercial insurance and established often to take advantage of favorable tax and other benefits[502]
Insurer	The company that indemnifies losses and often helps manage risk; a mutual insurer is one owned by and operated for the insured policyholders as opposed to a stock company that is owned by the general public
Producer	An agent or broker who sells insurance
Reinsurer	An insurer who in return for premiums accepts the liabilities of another insurance company that has ceded part or all of an insurance contract
Underwriter	An individual who is responsible for making decisions for an insurer on the acceptability of the terms of an insurance contract

Source: IRMI Risk & Insurance, “Glossary of Insurance and Risk Management Terms”

Select Types of Insurance Products

Admitted vs. Excess & Surplus (E&S) Lines	Admitted lines are regulated by state insurance commissioners. Policies are written by standard (or admitted) carriers. E&S lines have "freedom of rate and form" to adapt to the needs of customers — mainly businesses, but also some consumers. Policies are written by insurers that are not required to obtain state certification, but states do review and admit insurers.
Business Owners Policy (BOP)	Insurance for small/medium businesses that covers property (including business interruption insurance) and casualty but not workers compensation and specialty lines.
Commercial vs. Personal Lines	Commercial lines serve businesses and cover property/casualty and numerous specialty lines of insurance; personal lines serve individuals and cover life, health and property/casualty insurance (e.g. auto, home).
Commercial: Property vs. Casualty	Property insurance covers the owner or user of a property for the loss of that property and its associated income-producing ability (business interruption); coverage for an insured's direct losses is called first-party coverage. Casualty insurance, sometimes called general liability insurance, addresses losses associated with injuries to third-parties (known as third-party coverage) and covers legal liability, property damage, and injuries.
Commercial: Specialty Lines	These are insurance product lines that are less standard and include special liabilities, such as: professional liability insurance for errors and omissions (E&O) that covers financial losses to third parties for professional services wrongly performed; directors and officers liability (D&O) that can include, for example, coverage for acts and misstatements that lead to employment practices liability claims or shareholder lawsuits. Certain industry lines, such as for marine or aircraft, and for certain risks, such as for cyber risks, can also be specially covered.
Commercial: Surety bonds	A contract in which the insurer guarantees the performance of the insured.

Sources: American Association of Managing General Agents, "Excess and Surplus Lines FAQ's"; Insurance Information Institute, Insurance Handbook; IRMI Risk & Insurance, "Glossary of Insurance and Risk Management Terms"

The multi-state regulation of insurance makes for a complex system in the United States that is difficult to engage. The National Association of Insurance Commissioners (NAIC) is the national group working to assist state regulators. However, its mission statement, including protecting the public interest, may not apply as heavily to the public's national and international interests.[503]

Federal power grew in a small but important way with the establishment of the Federal Insurance Office (FIO) within the Department of the Treasury, as mandated by the 2010 Dodd-Frank legislation. The legislation reserved the states' rights on rates and most policy matters but allowed the FIO to preempt state policies if insurers in countries with which the US had

insurance agreements were not being treated on par with domestic insurers in doing US business.[504] The legislation also called for certain studies of the US system.

A December 2013 study by the FIO noted the challenges of diffuse oversight: "The absence of uniformity in the US insurance regulatory system creates inefficiencies and burdens for consumers, insurers and the international community."[505] The report recommended that all states participate in the Interstate Insurance Product Regulation Commission, which seeks policy standardization on selected consumer policies, and develop standardized forms and terms for commercial lines.[506] In discussions with the project team, insurance brokers and agents raised those same issues as impediments to effective term comparison across policies. The FIO report also recommended that the federal government facilitate the adoption of selected national standards, such as for licensing of insurance producers.

Despite states not liking increased federal involvement, it is key for US participation in international efforts to have a single, federal point of contact in the FIO. This is all the more important given the trend toward standardization and more multilateral cooperation and agreements. For example, the FIO convened US and EU insurance leadership to initiate the EU-US Insurance Project in order to "promote business opportunity, consumer protection, and effective supervision."[507] The FIO receives support and advice from the Federal Advisory Committee on Insurance (FACI), whose members include selected insurance commissioners, private sector insurers and researchers.[508]

The insurance industry also has to comply with extensive US laws and regulations governing commercial business, including sanctions enforcement in the international marketplace. The Treasury Department's Office of Foreign Assets Control (OFAC) provides guidance to the industry.[509]

Different parts of government also interact with the insurance industry in ways beyond regulation. The Treasury Department administers the Terrorism Insurance Act (TRIA) program, to support underwriting of terrorism risk.[510] The Federal Emergency Management Agency, part of DHS, works on certain risk management issues, such as flood insurance. DHS also interacts with the industry through the information-sharing programs of its critical infrastructure program. The insurance industry is considered part of the Financial Services Sector, one of the 16 defined critical infrastructure sectors.

Only recently has government looked more broadly at insurance and considered how it could be used more directly to assist in motivating risk-reduction actions. A DHS pilot project is underway in partnership with the insurance industry to test market interest in building structural standards. DHS is also working with some in the insurance industry to consider how cyber standards can be used by the insurance industry in developing and pricing its new cyber-insurance products.

EXAMPLES OF HOW INSURANCE AFFECTS ILLICIT COMMERCE

The insurance industry has had a curious role in the Iran sanctions story. The sanctions had major effects on the shipping industry through sanction restrictions on property insurance (from cargo to hull) and on marine liability, known as the Protection & Indemnity (P&I) insurance cover.[511] Some of this coverage is required by international conventions, such as on environmental liabilities.[512] Iranian trade was stymied not only by direct sanctions on certain entities and products but also by these prohibitions on P&I cover for ship operations, which carriers could not get if transporting Iranian oil. But markets adapt. With some of the large UK and other P&I insurers out of the market, new marine insurance appeared, with Iran issuing sovereign cover and with other P&I cover appearing from markets in Russia, China, India and Japan[513] (the latter two having limited waivers for oil shipments).[514]

Strict sanctions on Iran — sanctions that primarily target Iran's key energy sector and its access to the international financial system — harmed Iran's economy to the point where Iran's leaders, on November 24, 2013, accepted an interim agreement the thrust of which is to halt further expansion of Iran's nuclear program in exchange for apparently modest sanctions relief.

Kenneth Katzman
Congressional Research Service
"Iran Sanctions"
June 2014

Nonetheless, the restrictions on insurance caused enough of a market hiccup to have some effect. The easing of Iranian sanctions may cause some to look to get back into that market, but caution is the watchword — as major insurance claims can take years to work out and the sanctions may be only temporarily lifted. One major problem for US firms is the continuing changes envisioned for the Iran sanctions regime, with changes resulting from international negotiations. As one Iran sanctions specialist noted, "Iran has become kryptonite for banks and shippers and insurance companies."[515] As insurers manage their own risks, they consider the potential cost to their business overall.

Some in the insurance industry told the project team of frustration when asking for operating guidance from the US government. For example, although the Treasury Department provides enforcement guidelines for its application of sanctions penalties, so much of the interpretation of the guideline may depend on who within a department answers the question: Is this *de minimis*?[516] The project team found that companies are very hesitant to contact government with questions. They fear government will respond by "asking" them to open their books and engage in a time-consuming inquiry.

Insurance for tankers to export Iranian crude may be unusable even after the U.S. and the European Union eased sanctions against the Persian Gulf state, a group covering vessel owners said. Ship owners hauling Iran's oil may go unpaid if they claim against insurance policies after July 20 [2014], the date temporary relief of sanctions on the nation is due to expire or be renewed…The Office of Foreign Assets Control, part of the U.S. Treasury, declined to clarify whether claims would be recoverable after July even if the incident happened before then…

Alaric Nightingale, Bloomberg News
"Iran Oil-Shipping Insurance Seen Unusable on Lack of Clarity"
January 28, 2014

OFAC actions against the insurance industry are not frequent, nor are the penalties large. For example, in 2011, Aon remitted $36,000 to settle Iran sanctions violations committed in 2005.[517] Additionally, the American Club, a mutual protection and indemnity association, was fined $348,000 (twenty percent of the base penalty). While it did not voluntarily self-disclose, the company was a "first-time" offender in its sanctions violations related to processing insurance claims.[518]

But the effort that goes into any company managing an investigation or responding to a government inquiry and also increasing its internal compliance program can be substantial, companies, lawyers and the government told the project team. Given the magnitude of the insurance industry's international transactions, the insurance industry has not been hit hard with fines — but compliance can be costly in time, systems investment and potential for lost business. Even when sanctions are loosened, as is the case with Iran, companies are loathe to change their compliance systems once established, as any changes or errors could prove costly.

Sanctions are important national security policy instruments, as are export controls. In terms of insurers' oversight of companies they insure, intermediaries like insurance companies cannot insure illegal acts. The exporter has to attest to the material it is shipping, the legality of the shipment and its value. Insurers also simply put standardized sanctions clauses in their insurance contracts.[519] Similar clauses relate to export controls and other illegal acts. Notably, although insurers may not cover government fines and penalties, they can cover costs associated with these, such as defending against government actions.

The following table further explores the nexus between the insurance industry and trade stakeholders. It illustrates how insurance needs are related to national security interests and how this relationship might be better used to the advantage of both the private sector stakeholder and public sector interests. Potential exists for using certain insurance lines, such as Errors & Omissions (E&O) insurance, or creating new types of insurance products, such as compliance insurance, from which both the private and public sectors could benefit.

Trade Stakeholders, Security Concerns and Insurance Protections

Stakeholder	Relevant Security Concerns	Insurance Lines
Exporters	Export controls and sanctions compliance; intellectual property theft	Directors & officers (D&O); cyber; compliance insurance (potential new product)
	Export controls, sanctions, foreign corrupt practices, etc.	Compliance insurance (potential new product)
Port operators	Business continuity and terrorism risk coverage; thefts, tampering and diversions; insider sabotage	Property and casualty, including business continuity and cyber
Logistics service providers	Export controls and sanctions compliance; piracy	Errors and Omissions (E&O); cyber; surety bonds (potential on exports)
Carriers (air, ground, ocean, rail)	Numerous and varied	Selected: property, cyber, marine, protection & indemnity (P&I), etc.

However, the challenge of accurate risk pricing has stymied the development of some insurance lines. International trade involves many different types of insurance and insured losses. These range from property theft or vandalism of shipping containers at ports, to diversion of goods through the use of cyber identity theft on truckers' load boards, to cargo and hull losses from natural disasters or piracy.[520]

In industry discussions, the project team learned that much of the insurance industry lags rather than leads in areas of enterprise development, that insurance companies do not always price based on risk, that policy terms, which are risk-based, can be very subjectively set, and that the industry generally responds by exiting areas of risk where uncertainties are high. Thus, using the insurance industry as a motivator to reduce risks of illicit trade may face challenges — but it can be done.

While insurance providers include exclusions in their policies for illegal transactions by their customers, they do have a general interest in an overall safer world. Among other objectives, insurers support:

- Less illicit trade, which means more legal trade and more opportunities to see insurance
- A lower risk world, which would mean fewer claims
- A less volatile risk environment so that insurers could better estimate risk through modeling and predictive analytics

Some in the insurance industry have been specifically active on the issue of climate change, as that more directly affects an insured's risks.[521]

Insurers do underwrite various risks of exporters and logistics service providers. Exporting companies and logistics service providers have their own liabilities stemming from due diligence requirements under sanctions regimes, export controls and other laws and regulations. Entities have to comply with a multitude of requirements, from hiring practices to safety rules, from the US Foreign Corrupt Practices Act to importing country requirements. These customers finding no clear standards in place for some of their risks, wonder what constitutes "due diligence" and how much compliance is enough.

All firms have to comply with these many government requirements. Major exporters are typically large firms that have Directors & Officers (D&O) liability insurance. D&O policies cover the costs of defending even wrongful acts and criminal proceedings, but they do not cover fraud, intentional non-compliance, or illegal gains. In the United States, D&O customers pay about $6 billion in annual premiums, and coverage costs are trending up.[522] Given that foreign firms are also subject to US export controls and sanctions, overseas companies have been advised to make sure their D&O covers defense against US actions.[523]

Compliance officers for major exporters want relief. Their activities are now considered cost centers that are not only costly unto themselves (with inside and outside legal counsel) but also hold up business transactions. They would like to see:

- Clear compliance standards that are built on – or at least harmonized with – best practices developed by industry
- The ability to outsource at least part of compliance to third parties

Logistics service providers would also like some clearer compliance standards. Some, such as freight forwarders, have become export compliance advisors, particularly for smaller companies and sometimes by default — as they have to educate smaller exporters on export controls and sanctions.[524] These providers have an obligation not to ship to prohibited persons or places but generally rely on the exporter to ensure compliance with classification of the export and identification of any licensing requirements.

Some freight forwarders have been assessed penalties, generally for facilitating shipments to "prohibited persons or places." Routed export transactions are a particular source of risk for transportation service providers; when they act as agent with power of attorney, they become the exporter. However, all forwarders bear some responsibility under "know your customer" requirements and need to have a system in place to alert to red flags.[525]

These logistics service providers and other trade facilitators and advisors to companies have professional liability insurance to cover errors they make in their work that would lead a company to be penalized. A recent judgment, for example, against one exporter noted that the company, which was fined many millions of dollars, had relied upon the erroneous advice of a professional consultant that a product was not subject to International Traffic in Arms Regulations (ITAR). The exporter could claim that the advisor was professionally negligent and seek recompense. If the consultant had been a freight forwarder with errors and omissions (E&O) insurance or an attorney with malpractice insurance, the insurer would be involved.

The general counsel of the company that was fined, however, told the project team that the company had not sought any recompense from the advisor. The general counsel said he thought the advisor was a good one and would even be willing to use the advisor again because he considered the government judgment wrong. He noted, however, the lack of professional standards in trade compliance consulting.[526]

Industry — from exporters to logistics service providers to insurance industry professionals — consistently told the project team of the need for more specific compliance standards. Otherwise, they said, how are they to know how much compliance is enough? Could some aspects of compliance be outsourced with some sort of "blessing" from the government?

There are few external pressures to validate export compliance other than the potential government penalties or reputational losses, if any, and only discussion of a potential industry code of conduct.[527] The Coalition for Excellence in Export Compliance (CEEC) has been working to develop best practices, but these are not yet government-recognized. Dun & Bradstreet is developing a suite of company compliance products that the project team suggested should include some end-user verification rating standards. The project team discussed this concept with similar firms. For such a tool to gain significant buy-in from industry, government would have to acknowledge what constitutes due diligence and end-user verification.

General Counsels and other exporter compliance officials have supported the possibility of the development of more robust insurance to cover compliance that would be predicated on government and industry coming to an agreement on more explicit standards.

More Targeted Government Market Interventions

Direct government intervention in insurance markets generally occurs when the insurance industry has either exited a market or not provided insurance coverage that the government decides should be provided to increase the societal good. These interventions have occurred both at the federal and state levels.

At the state level, California requires insurers who offer homeowners insurance policies to offer earthquake insurance.[528] Faced with similar private insurance industry qualms on hurricanes, Florida established a non-profit, Citizens United Insurance Corporation.[529]

At the federal level, the government has directly intervened in the market for both terrorism risk and flood insurance; in both cases when the private market appeared unwilling to extend what was deemed sufficient coverage due to potentially catastrophic, difficult-to-predict risks. It is now considering insurance and liability incentives with the industry in discussions on cyber insurance. Both the terrorism risk and the cyber risks are discussed earlier in this report.

In 1968, Congress established the National Flood Insurance Program to reduce property lost to flooding and government spending on disaster compensation. The Federal Emergency Management Agency (FEMA), which administers the program, estimates that $1.6 billion is saved each year due to buildings being constructed to the program's flood standards and communities instituting land-use zoning.[530] However, due to some catastrophic floods,

historically subsidized premiums for much of the program, and some homeowner non-compliance with requirements to purchase flood insurance, the program has faced high losses.[531]

New flood mapping and some adjusted premium rating are leading to substantial increases in premiums to more closely reflect risks. Second homes and businesses will no longer be eligible for subsidized rates.[532] Some note that more adjustments to the program are needed in order to give appropriate credits to reflect risks,[533] and that issues of equity and affordability need to be addressed in order to ensure that the division between public and private sector interests be more clearly addressed for catastrophic risks.[534]

A January 2014 GAO report looked at the potential for broader homeowners insurance, noting the federal government payout for Superstorm Sandy had been over $7 billion under National Flood Insurance claims (not including disaster assistance). The GAO also underscored the need for cooperation among government, industry and homeowners to address various challenges. The report concluded: "The possibility of improved data, better risk modeling, and emerging private-sector interest, however, suggest that some additional coverage may be possible. For this to happen, private insurers must be able to assess and diversify risk and charge rates adequate for the risk they are assuming."[535]

Changes are afoot not only in the flood insurance program but also in the terrorism risk program, which is set to expire at the end of 2014. To the extent possible, underwriters build relevant risks into the terms under which they offer terrorism risk coverage. Some also choose to cap their exposure to high-terrorist-target markets. However, to provide better "risk validation," some insurance providers have argued for significantly increasing the loss trigger above $100 million and charging a reinsurance fee upfront (rather than via a recapture provision) for the government backstopping as well as other changes — including perhaps allowing the TRIA program to expire and private market pricing to prevail.[536]

Most in the insurance industry would agree that some adjustments to the TRIA program would be useful to the marketplace and security, but that terminating the program would not make sense. The think tank Rand has found that for terrorist attacks resulting in losses of $40-60 billion, TRIA saves government money due to industry retention of some losses, recoupment from insurers of some government payouts, and displacement of some inevitable federal disaster assistance.[537] Another Rand report notes: "Access to appropriately priced terrorism insurance can promote economic growth, making resources available to address national security threats or other social problems."[538] To be sure, there are major obstacles to appropriate pricing.

An argument against continued government reinsurance cites increased capacity in the market for managing catastrophic risks. Some observers say that alternative financing mechanisms, in particular, are under-appreciated. Insurance-linked securities, for example, offer a means for insurers and reinsurers to cope with regulations on their reserve requirements and manage large risks.[539]

Another class of alternative finance mechanism is catastrophe bonds, also known as Cat bonds. These are high-yielding obligations in which investors receive a payment in exchange for pay out in the event of pre-defined catastrophes.[540] These bonds are increasing in the market but are generally for modelled risks with good actuarial data, such as hurricanes.[541] The catastrophe bond outstanding capacity is about $14 billion.[542] For terrorism, reinsurance capacity is

estimated at no more than $10 billion in the US, and in such cases Cat bonds cannot come to the rescue.[543] They have generally been issued for specific events or for pools of risk and have not been generally available for underwriting such risks for on-going businesses.[544]

As noted in the earlier section on US market interventions, terrorism risk insurance is important to trade as it is used by stakeholders across the supply chain, such as port authorities.

Explicitly including nuclear, biological, chemical and radiological (NBCR) coverage has been considered but has not yet been addressed sufficiently.[545] Some risk management experts support adding such coverage in the TRIA expansion. As the Risk and Insurance Management Society (RIMS) explains:

> The current TRIA program neither explicitly includes nor excludes NBCR events, which has prompted many insurers to exclude NBCR events from terrorism policies based on long-standing standard exclusions for nuclear and pollution risks…As a result consumers are generally unable to obtain NBCR coverage. RIMS supports the inclusion of NBCR coverage in a long term extension of the TRIA program. NBCR events have a high probability of resulting in catastrophic losses for organizations affected by such an attack.[546]

Covering catastrophic cyber events under TRIA or similar legislation also needs to be considered.[547]

Government typically provides support to companies after a disaster or a market collapse. However, more proactively engaging with the insurance industry to discover broader areas of national security concern would make sense. In the US today, government engagement with the insurance industry is fragmented. No one today is looking systematically for ways to help the insurance industry obtain needed risk information, assess client performance, and more accurately signal risk to the market across areas of concern. The industry is more ready for this today than it was a decade ago.

RISK-BASED PRICING?

A decade ago, when leaders of the newly created US Department of Homeland Security (DHS) were investigating how to streamline a very complex set of risk management processes, they sought out the insurance industry. Considering how to evaluate chemical industry risks and incentivize tighter security, DHS officials said to insurance industry representatives, "You can do this so we don't have to!" The insurance association executive laughed, recalling the incident. DHS learned that actual risk evaluations are just one small part of what goes into insurance pricing.[548] Or at least that is the way it has been until now.

In the United States, states oversee insurance policy pricing, with some having statutory requirements on rates and practices. Although personal insurance lines are heavily reviewed, commercial property-casualty line rates are more independently set.[549]

The structure and pricing of commercial policies is complex, with insurance industry rates driven by company overall business performance in its commercial environment. Insurance companies charge premiums that are expected to cover some future expected payout, but many other factors go into managing the insurance business and commercial relationships. This

includes ceding parts of premiums and book of business to reinsurers and other investors who will share in the underwriting of the risk as well as managing the capital balances reserved for future payout. The insurance package of policy terms (premiums, deductibles, exclusions, and limits) change and are not just related to risk, especially in the commercial markets and specialty lines.

In addition, insurance-linked securities have developed. These are fixed income vehicles that give off higher yields due to their higher risks and are not generally tied to market returns. This burgeoning speculative market has become a source of additional funding in the insurance market — but one that is less directly linked to the underlying risks of the insurance policies and therefore not as reflective of the risk. Regulators worry about the systemic risks that can unfold in this market.

Commercial insurance producers told the project team that they have pricing leeway and evaluate customers on the full potential of the business relationship. Much effort goes into evaluating the insured's needs, developing the scope of insurance to place, completing the forms to get estimates from underwriters (who inevitably want more information and each one with different information than that on the industry-standard ACORD forms) and then working again with the client. This will cause some brokers not to work with smaller accounts, who then have to scramble to find coverage they want.

Insurance carriers accordingly don't rely solely on technical compliance with existing information security standards when assessing a company's qualifications for cybersecurity insurance coverage. Many instead examine its risk culture...

DHS *Cyber Risk Culture Roundtable Readout Report*
May 2013

From the buyer's point of view, commercial insurance providers offer more tailored products than personal insurance providers. According to an industry specialist, this may be good for the companies who want products tailored to their needs but also works to the advantage of insurers by reducing the ability of the insured to compare policy packages.

Technology and data are also changing commercial insurance today. Predictive analytics — in which risks are considered more specifically — is seen as helping to drive insurance profits in an increasingly competitive, global marketplace. While recognizing that capital returns will always be a major part of insurance industry profit performance, insurers are increasingly looking at what data will drive future losses.[550]

US insurers are increasing technology spending. According to Insurance Networking News, "Among the top 10 projects identified were analytics, business intelligence, data warehousing and big data, all intended to help insurers make better use of the data they have, access newly available data and make better, more informed decisions to find opportunities, price them more effectively and reduce losses."[551]

Despite the pending revolution in business from big data and analytics,[552] IT research company Gartner predicts that through 2015 the vast majority of Fortune 500 companies will not be able

to use big data well.[553] The Tower Watson [Property and Casualty] Insurance Predictive Modeling Survey, carried out in 2012, showed that the personal line and the smaller and mid-market commercial line carriers were using predictive analytics more than the insurers of large commercial accounts and specialty lines; this may have been due to large legacy IT systems being hard to change.[554] How insurers use all the data also differed.

Attendees at the DHS cyber insurance panels were reserved on predictions for predictive analytics driving reduced risks, noting problems due to insufficient numbers of analysts, questions over modeling accuracy, and general inexperience yet with big data.[555] On cyber insurance, they noted the need for the development of common cybersecurity standards and best practices and a better understanding of the scenarios that could cause losses.[556]

The read-out from a November 2012 DHS cyber panel noted that one option for incentivizing the insurance industry to develop new products in the national security interest would be to pass "a 'Cyber Safety Act,' modeled on the SAFETY Act. Its goal would be to promote the development of: (1) new cybersecurity-enhancing technologies and services; (2) insurance requirements for purchasers of those offerings; and (3) corresponding liability caps."[557]

Industry associations are supporting the move towards standards and the use of analytics. The American Association of Insurance Services, for example, already provides standard policies for a wide variety of personal insurance products and is addressing emerging exposure in property and liability insurance.[558] It has developed a cloud-based rating engine that insurers can adapt to their needs.[559] The work of the Institute for Business and Home Safety, cited earlier, is an example of industry developing standards to apply to building resilience, which governments can also use. However, government can consider national security challenges more broadly — including on nonproliferation concerns — and engage industry in developing ways to incentivize changes in liability schemes, including insurance-based risk management incentives.

---

[438] American National Standards Institute (ANSI). "ANSI: Historical Overview." Accessed January 6, 2014. http://www.ansi.org/about_ansi/introduction/history.aspx?menuid=1.

[439] ANSI. "Through History with Standards." Accessed January 6, 2014. http://www.ansi.org/consumer_affairs/history_standards.aspx.

[440] Institute of Nuclear power Operations (INPO). "About Us." Accessed January 11, 2014. http://www.inpo.info/AboutUs.htm#history.

[441] WANO. "History." Accessed January 30, 2014. http://www.wano.info/about-us/history.

[442] National Fire Protection Agency (NFPA). "The Birth of NFPA." NFPA History. Accessed January 14, 2014. http://www.nfpa.org/itemDetail.asp?categoryID=500&itemID=18020.

[443] Insurance Institute for Business & Home Safety. "Insurance Institute for Business & Home Safety Research Center." Accessed January 13, 2014. http://ofb.ibhs.org/content/data/file/RSC_overview_020112.pdf.

[444] University of Denver. "Global Efforts: ANSI/ASIS International Standards." University of Denver Sie Cheou-Kang Center Private Security Monitor. Accessed January 6, 2014. http://psm.du.edu/international_regulation/global_standards_codes_of_conduct/asis_standard.html.

[445] Groupe EYSSAUTIER. "Germany to Introduce Compulsory Liability Insurance for Ship Security Firms." Last modified July 2, 2013. Accessed December 12, 2013. http://www.groupe-eyssautier.com/fr/actualites/revue-de-presse/germany-to-introduce-compulsory-liability-insur.html.

[446] International Organization for Standardization (ISO). "ISO Survey." Accessed January 8, 2014. http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO%209001&countrycode=AF.

[447] Ibid.

[448] ANSI. "About ANSI Overview." Accessed January 6, 2014. http://www.ansi.org/about_ansi/overview/overview.aspx?menuid=1.

[449] US DHS. FEMA. "About PS-Prep™." Last modified November 5, 2013. Accessed December 13, 2013. http://www.fema.gov/about-ps-preptm.

[450] International Organization for Standardization (ISO) . "About ISO." Accessed May 1, 2014. http://www.iso.org/iso/home/about.htm

[451] *ISO 28000:2007: Specification for security management systems for the supply chain*. ISO. December 17, 2010. Accessed May 1, 2014. http://www.iso.org/iso/catalogue_detail?csnumber=44641

[452] In the words of ISO Secretary-General Alan Bryden: "Threats in the international market-place know no borders. The ISO 28000 series provides a global solution to this global problem. With an internationally recognized security management system, stakeholders in the supply chain can ensure the safety of cargo and people, while facilitating international trade, thus contributing to the welfare of society as a whole." See: ISO. "New suite of ISO supply chain management standards to reduce risks of terrorism, piracy and fraud." Last modified October 25, 2007. Accessed May 1, 2014. http://www.iso.org/iso/news.htm?refid=Ref1086.

[453] Ibid.

[454] TAPA utilizes a compliance certification program to ensure standards. Companies and insurers are increasingly using TAPA certification as a prerequisite for use. The ultimate goal is that shipping companies will be forced to seek TAPA certification in order to be competitive. The standardization has also been successful because of TAPA's cooperation with the U.S. Government, which uses the standards as the basis for minimum homeland security compliance. See: Transported Asset Protection Association (TAPA). "Standards." Accessed May 1, 2014. http://www.tapaonline.org/standards.

[455] Ibid.

[456] Ibid.

[457] ASIS International. "Under Development." Standards. Accessed May 2, 2014. https://www.asisonline.org/Standards-Guidelines/Standards/under-development/Pages/default.aspx

[458] ASIS International. "Resilience in the Supply Chain Standard (SPC.3)." Standards. Accessed May 2, 2014. https://www.asisonline.org/Standards-Guidelines/Standards/under-development/Pages/Resilience-in-the-Supply-Chain-Standard.aspx

[459] ASIS International. "Supply Chain Risk Management Standard: A Compilation of Best Practices (SCRM)." Standards. Accessed May 2, 2014. https://www.asisonline.org/Standards-

Guidelines/Standards/under-development/Pages/Supply-Chain-Risk-Management-Standard-Compilation-of-Best-Practices.aspx

[460] Coalition for Excellence in Export Compliance (CEEC) . "CEEC Introduction." Accessed April 10, 2013. http://www.ceecbestpractices.org/best-practices-standards-workgroup.html

[461]National Foreign Trade Control (NFTC). "A Cheat Sheet to the WTO Trade Facilitation Agreement." Washington, DC: NFTC, last modified December 2013. Accessed December 19, 2013. http://www.nftc.org/default/Publications/Trade_Policy/WTO%20Trade%20Facilitation%20Agreement%20%20Cheat%20Sheet.pdf.

[462] This includes a provision that "[e]ach Member shall, to the extent practicable and in a manner consistent with its domestic law and legal system, provide opportunities and an appropriate time period to traders and other interested parties to comment on the proposed introduction or amendment of laws and regulations of general application related to the movement, release and clearance of goods, including goods in transit." See World Trade Organization. *Agreement on Trade Facilitation*. Report no. WT/MIN(13)/W/8. Ministerial Conference, 9th sess., Bali: December 8, 2013: 3. Accessed December 20, 2013. https://mc9.wto.org/system/files/documents/w8_0.pdf.

[463] US DOC. Bureau of Industry and Security. Office of Technology Evaluation. *BIS "Best Practices" for Industry to Guard Against Unlawful Diversion through Transshipment Trade*. Washington, DC: DOC, July 2012: 1–2.

[464] Ibid., 24.

[465] DOC. Census Bureau. *Automated Export System*: Best Practices. October 2013. 4.

[466] DOC. Census Bureau. "Foreign Trade Regulations: Mandatory Automated Export System Filing for All Shipments Requiring Shipper's Export Declaration Information." *Federal Register* 78, no. 50 (March 14, 2013). Accessed April 14, 2014. http://www.gpo.gov/fdsys/pkg/FR-2013-03-14/pdf/2013-05435.pdf.

[467] GS1. "GS1 Timeline." Accessed May 2, 2014. http://www.gs1.org/about/media_centre/timeline

[468] GTIN Info. "GTIN Information: Definition."

[469] World Customs Organization. "Cooperation between WCO and GS1 highlighted at GS1 Global Forum 2013." Last modified Feburaruy 2013. Accessed May 2, 2014. http://www.wcoomd.org/en/media/newsroom/2013/february/cooperation-between-wco-and-gs1.aspx.

[470] For example, the GS1 Global Data Synchronization Network stores information on imports in a cloud-based platform that allows governments and a variety of agencies to access potentially valuable information. See: *GS1 GDSN: Proven Benefits for Trading Partners.* GS1. 2008. Accessed May 1, 2014. http://www.gs1.org/docs/gdsn/GDSN_Overview.pdf.

[471] ITDS. "The Business Case for Using E-Commerce Data to Manage Product Admission at International Borders." Washington, DC: ITDS, December 2011: 1. Accessed December 19, 2013. http://www.itds.gov/linkhandler/itds/tsn/draft_trade_comment.ctt/draft_trade_comment.pdf.

[472] Rowden, "Comments on ITDS Product Information," 2.

[473] International Air Transport Association. "Secure Freight: A Supply Chain Security Program." Cargo Security. Accessed December 19, 2013. http://www.iata.org/whatwedo/cargo/security/Pages/secure-freight.aspx.

[474] Market Watch: Wall Street Journal. "INTTRA Releases March Results of Ocean Shipping Information Quality Program." Last modified April 10, 2014. Accessed April 14, 2014. http://www.marketwatch.com/story/inttra-releases-march-results-of-ocean-shipping-information-quality-program-2014-04-10.

[475] RightShip. "About RightShip." Accessed April 14, 2014. http://site.rightship.com/about/who-we-are/.

[476] Kunreuther, Howard C., Stacy McMorrow, and Mark V. Pauly. *Insurance and Behavioral Economics: Improving Decisions in the Most Misunderstood Industry*. Cambridge, UK: Cambridge University Press, 2013.

[477] DHS. "Engineering Resilience: The Resilience STAR™ Home Pilot Project." Last modified November 18, 2013.Accessed December 6, 2013. http://www.dhs.gov/blog/2013/11/18/engineering-resilience-resilience-star%E2%84%A2-home-pilot-project.

[478] US Department of Housing and Urban Development (HUD). *Hurricane Sandy Rebuilding Strategy*. August 2013.

[479] Author interview with DHS executive. Washington, DC. January 2014.

[480] Author interviews. Washington, DC. February 2014.

[481] International Council of Chemical Associations (ICCA). "Responsible Care." Accessed January 7, 2014. http://www.icca-chem.org/en/Home/Responsible-care/.

[482] Bond, Sam. "Cyanide spill nets Czech chemical company hefty fine." edieWaste, January 18, 2006. Accessed January 17, 2014. http://www.edie.net/news/3/Cyanide-spill-nets-Czech-chemical-company-hefty-fine/10985/.

[483] Chemical Industry Archives. "Responsible Care: Results." Last modified March 27, 2009. Accessed January 7, 2014. http://www.chemicalindustryarchives.org/dirtysecrets/responsiblecare/6.asp.

[484] Muse, Roger. "What's in a Name: Accreditation vs. Certification?" Quality Magazine, June 2, 2008. Accessed December 18, 2013. http://www.qualitymag.com/articles/85483-what-s-in-a-name-accreditation-vs-certification.

[485] International Organization for Standardization (ISO). "Certification to ISO Management System Standards." Accessed January 8, 2014. http://www.iso.org/iso/home/standards/certification.htm.

[486] Author discussion with a sttandards developer, 2013.

[487] RightShip. Interview with author. Washington, DC. 2013.

[488] Groupe EYSSAUTIER, "Germany to Introduce Compulsory Liability."

[489] ISO. "Creating Value from Your Assets — A New ISO Standard can Help." ISO News. Last modified December 10, 2013. Accessed January 15, 2014. http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1805.

[490] ISO. "ISO 31000 — Risk Management." Accessed January 15, 2014. http://www.iso.org/iso/home/standards/iso31000.htm.

[491] McNally, J. Stephen. *The 2013 COSO Framework & SOX Compliance: One Approach to an Effective Transition.* Committee of Sponsoring Organizations of the Treadway Commission, June 2013. Accessed December 14, 2013. http://www.coso.org/documents/coso%20mcnallytransition%20article-final%20coso%20version%20proof_5-31-13.pdf.

[492] Olshan. "SEC Staff Issues Report With Recommendations to Numerous Regulation S-K Disclosure Requirements." Olshan Articles & Alerts. Last modified January 2014. Accessed January 20, 2014. http://www.olshanlaw.com/resources-alerts-Client-Alert-SEC-Recommendations-SKDisclosure.html.

[493] White, Mary Jo. "'The Path Forward on Disclosure." Speech given at the National Association of Corporate Directors Leadership Conference, National Harbor, MD, October 15, 2013. Accessed December 17, 2013. http://www.sec.gov/News/Speech/Detail/Speech/1370539878806#.Uu-wMrSrDF8.

[494] Author discussions with companies and law firms.

[495] Author discussions with industry. See also: http://www.fcpablog.com/blog/tag/disclosure#

[496] http://www.gsnmagazine.com/article/25476/ice_says_public_tip_line_generates_investigative_l; http://www.naasca.org/2012-Articles/011812-ICE-TipLineGeneratesLeads.htm

[497] Organization for Economic Cooperation and Development (OECD). "Measuring Trade in Value Added: An OECD-WTO Joint Initiative." OECD Industry and Globalization. Accessed January 23, 2014. http://www.oecd.org/industry/ind/measuringtradeinvalue-addedanoecd-wtojointinitiative.htm.

[498] *Strategies for Managing Customer and Supplier Risks.* London: The Economist Intelligence Unit, 2013. Accessed January 6, 2014. http://www.economistinsights.com/sites/default/files/EIU%20D%26B%20paper%20FINAL%20Nov%2021%20with%20new%20logo.pdf.

[499] Insurance Information Institute. "Glossary." Insurance Tools. Services. Accessed August 11, 2014. http://www.iii.org/services/glossary/I.

[500] Decker, Debra K., and Erwann O. Michel-Kerjan. A New Energy Paradigm: Ensuring Nuclear Fuel Supply and Nonproliferation through International Collaboration with insurance and Financial Markets. Cambridge, MA: Harvard University Kennedy School of Government, March 2007. Accessed January 10, 2014. http://belfercenter.ksg.harvard.edu/files/decker_michel_kerjan_march_2007.pdf.

[501] Hartwig, Robert P. *The Historical Arc of Insurance Regulation and Modernization: Convergence or Disharmony? Past, Present and Future*. New York: Insurance Information Institute, October 24, 2013. http://www.iii.org/presentations/the-historical-arc-of-insurance-regulation-and-modernization-convergence-or-disharmony-past-present-and-future.html.

[502] Adkisson, Jay. "Ten Favorite Things About Captive Insurance Companies." Forbes, August 10, 2013. Accessed August 11, 2014. http://www.forbes.com/sites/jayadkisson/2013/08/10/ten-good-non-tax-things-about-captive-insurance-companies/.

[503] National Association of Insurance Commissioners (NAIC). "About the NAIC." Accessed January 10, 2014. http://www.naic.org/index_about.htm.

[504] Norman, Edward C. *The New Federal Insurance Office.* Malvern, PA: CPCU Society Regulatory & Legislative Interest Group, May 2012. Accessed January 7, 2014. http://www.naic.org/documents/cipr_fio_additional_resources_cpcu_fio_article.pdf.

[505] Improving Property and Casualty Insurance Regulation in the United States. Washington, DC: McKinsey & Company, 2009. Quoted in US Treasury. Federal Insurance Office. How to Modernize and Improve the System of Insurance Regulation in the United States. December 2013. Accessed January 5, 2014. http://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/How%20to%20Modernize%20and%20Improve%20the%20System%20of%20Insurance%20Regulation%20in%20the%20United%20States.pdf.

[506] Interstate Insurance Product Regulation Commission (IIPRC). "About the IIPRC." Accessed December 18, 2013. http://www.insurancecompact.org/about.htm.

[507] US Treasury. "EU-U.S. Insurance Dialogue Project." EU-U.S. Insurance Project. Federal Insurance Office. Initiatives. Last modified August 7, 2014. Accessed August 11, 2014. http://www.treasury.gov/initiatives/fio/EU-US%20Insurance%20Project/Pages/default.aspx.

[508] US Treasury. "FACI Members." Offices. Organizational Structure. About. Last modified August 5, 2014. Accessed August 11, 2014. http://www.treasury.gov/about/organizational-structure/offices/Pages/faci_members.aspx.

[509] US Treasury. "OFAC Information for Industry Groups." Financial Solutions. Resource Center. Last modified April 26, 2013. Accessed August 11, 2014. http://www.treasury.gov/resource-center/sanctions/Pages/regulations.aspx.

[510] US Treasury. "Terrorism Risk Insurance Program." Financial Markets, Financial Institutions and Fiscal Service. Resource Center. Last modified August 19, 2013. Accessed August 19, 2013. http://www.treasury.gov/resource-center/fin-mkts/Pages/program.aspx.

[511] UK P&I Club. "Introductory Guide to P&I Cover." About The Club. Accessed January 31, 2014. http://www.ukpandi.com/about-the-club/rules-cover/introductory-guide-to-pi-cover/.

[512] *An Introduction to P&I Insurance for Mariners.* Oslo: Skuld, 2009. Accessed June 31, 2014. http://www.fd.unl.pt/docentes_docs/ma/wks_MA_19719.pdf.

[513] Moran, Matthew, and Daniel Salisbury. *Sanctions and the Insurance Industry: Challenges and Opportunities*. London: King's College London, September 2013. Accessed December 10, 2013. http://www.kcl.ac.uk/sspp/departments/warstudies/research/groups/csss/pubs/insurancereport.pdf.

[514] *U.S. Issues Further Sanctions Waivers under the National Defense Authorization Act of 2012*. New York: Sidley Austin LLP, July 11, 2012. Accessed December 10, 2013. http://m.sidley.com/us-issues-further-sanctions-waivers-under-the-national-defense-authorization-act-of-2012-07-11-2012/.

[515] Gladstone, Rick. "Sanctions Are Eased; Iran Sees Little Relief." New York Times, April 13, 2014. Accessed August 11, 2014. http://www.nytimes.com/2014/04/14/world/middleeast/sanctions-are-eased-iran-sees-little-relief.html?hpw&rref=business&_r=1.

[516] "Economic Sanctions and Enforcement Guidelines." *Federal Register* 74, no. 215 (November 9, 2009): 57593-57608.

[517] US Treasury. *Enforcement Information for January 31, 2011.* January 2011. Accessed August 11, 2014. http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/02012011.pdf.

[518] For more information on the number of OFAC actions, see: Miller, Stephen A., Matthew A. Glazer, and Jeffrey M. Monhait. "Potential benefits of cooperation with OFAC (Part 2)." Inside Counsel, December 23, 2013. Accessed January 2, 2014. http://www.insidecounsel.com/2013/12/23/potential-benefits-of-cooperation-with-ofac-part-2; Moran and Salisbury, *Sanctions and the Insurance Industry*.

[519] Moran and Salisbury, Sanctions and the Insurance Industry.

[520] Trucking industry load boards match freight loads with truckers.

[521] *Signatories to the Carbon Price Communique — 2012-2014.* Cambridge, UK: The Corporate Climate Communiqués, 2014. Accessed August 11, 2014. http://www.climatecommuniques.com/Carbon-Price.aspx.

[522] *Introduction to D&O Insurance*. Munich: Allianz Global Corporate & Specialty, 2010. Accessed December 27, 2013. http://www.agcs.allianz.com/assets/PDFs/risk%20insights/AGCS-DO-infopaper.pdf.

[523] *Why do US Export Controls Affect Non-US Companies?* Leicester, UK: David Hayes Export Controls. Accessed February 1, 2014. http://www.partneringforcompliance.org/documents/dhayes_export_controls_non_us.pdf.

[524] Author interviews with freight forwarders.

[525] Alston & Bird, LLP. "Export Compliance for Freight Forwarders." Presentation given for the International Freight Forwarders and Customs House Brokers Association of Atlanta, Atlanta, GA, November 10, 2009. Accessed December 11, 2013. http://www.alston.com/files/Event/77fe7de1-8042-4480-92ad-17efadcc2973/Presentation/EventAttachment/98bc6ef0-f692-426f-a361-31e3fd32d0cc/Export%20Compliance%20for%20Freight%20Forwarders.pdf.

[526] Author interview with fined company.

[527] Some have argued that companies adopting a hypothetical exporters' code of conduct could derive reputational gains. See: Hund, Gretchen, and Amy Seward. *Industry Governance – Self Regulation to Address Nonproliferation and Nuclear Policy*. Seattle: Pacific Northwest National Laboratory, 2010. Accessed December 7, 2013. http://www.inmm.org/ScriptContent/PNNL/2010/Session%201%20-%20New%20Directions%20in%20Nonproliferation/Industry%20Governance%20-%20Self%20Regulation%20-%20%20G.%20Hund%20(PNNL)/Hund%20Paper%20INMM%203-16-10.pdf; Hund, Gretchen, and Andrew Kurzrok. "Beyond Compliance: Integrating Nonproliferation into Corporate Sustainability." *Bulletin of Atomic Scientists* 69, no. 3 (May/June 2013): 31-42.

[528] State of California. Department of Insurance. "Consumers: Earthquake Insurance." Last modified August 2013. Accessed December 10, 2013. http://www.insurance.ca.gov/0100-consumers/0060-information-guides/0040-residential/earthquake-insurance.cfm.

[529] Citizens Property Insurance Corporation. "Company Overview." About Us. Accessed December 12, 2013. https://www.citizensfla.com/about/generalinfo.cfm.

[530] LoC. CRS. *The National Flood Insurance Program: Status and Remaining Issues for Congress*. By King, Rawle O. February 6, 2013. Accessed August 11, 2014. http://www.fas.org/sgp/crs/misc/R42850.pdf.

[531] US Congress. Senate. Testimony of Alicia Puente Cackley on the National Flood Insurance Program: Hearing before the Committee on Banking, Housing, and Urban Affairs, Subcommittee on Economic Policy. 113th Cong., 1st sess., September 18, 2013. Accessed August 11, 2014. http://www.gao.gov/assets/660/657939.pdf.

[532] Ibid.

[533] Anderson, Jenny. "Outrage as Homeowners Prepare for Substantially Higher Flood Insurance Rates." New York Times, July 28, 2013. Accessed January 13, 2014. http://www.nytimes.com/2013/07/29/nyregion/overhaul-and-a-hurricane-have-flood-insurance-rates-set-for-huge-increases.html.

[534] Michel-Kerjan, Erwann, and Howard Kunreuther. "Paying for Future Catastrophes." New York Times, November 24, 2013. Accessed December 13, 2013. http://www.nytimes.com/2012/11/25/opinion/sunday/paying-for-future-catastrophes.html.

[535] GAO. *Homeowners Insurance: Multiple Challenges Make Expanding Private Coverage Difficult*. January 2014. Accessed January 29, 2014. http://www.gao.gov/assets/670/660531.pdf.

[536] Lehmann, R.J. "R Street's Csiszar recommends shifting more terrorism risk onto private market." R Street, November 13, 2013. Accessed December 2, 2013. http://www.rstreet.org/news-release/r-streets-csiszar-recommends-shifting-more-terrorism-risk-onto-private-market/; Rhee, Robert J. "The Terrorism Risk Insurance Act: Time to End the Corporate Welfare." CATO Institute Policy Analysis, no. 736 (September 10, 2013). Accessed January 9, 2014. http://object.cato.org/sites/cato.org/files/pubs/pdf/pa736_web_1.pdf.

[537] LaTourrette, Tom, and Noreen Clancy. *The Impact on Federal Spending of Allowing the Terrorism Risk Insurance Act to Expire*. Santa Monica, CA: RAND Corporation. 2014. Accessed August 11, 2014. http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR611/RAND_RR611.pdf.

[538] Willis, Henry H., and Omar Al-Shahery. *National Security Perspectives on Terrorism Risk Insurance in the United States.* Santa Monica, CA: RAND Corporation. 2014. Accessed August 11, 2014. http://www.rand.org/content/dam/rand/pubs/research_reports/RR500/RR573/RAND_RR573.pdf.

[539] See, e.g., the development of life insurance securitizations in: Shwachman, Perry J., Anthony J. Ribaudo, and R. Bradley Drake. *A new age: life insurance securitisation*. New York: Sidley Austin LLP, 2008. Accessed January 15, 2014. http://www.sidley.com/files/Publication/471793b9-a01b-4f2b-b31c-01cb52b18901/Presentation/PublicationAttachment/9f370e0d-7862-48b3-9b78-064a19fde826/p47-50%20IISR%20-%20A26_Sidley.pdf.

[540] Risk Management Solutions (RMS). *Cat Bonds Demystified: RMS Guide to the Asset Class.* Newark, CA: RMS, 2012. Accessed December 10, 2013. http://riskinc.com/Publications/Cat_Bonds_Demystified.pdf.

[541] Artemis. "RMS models $1.2 billion of 2013 catastrophe bonds." Artemis, May 2, 2013. Accessed January 8, 2014. http://www.artemis.bm/blog/2013/05/02/rms-models-1-2-billion-of-2013-catastrophe-bonds/.

[542] Artemis. "Outstanding catastrophe bond capacity close to all-time highs: Willis." Artemis, June 12, 2012. Accessed August 13, 2014. http://www.artemis.bm/blog/2012/06/12/outstanding-catastrophe-bond-capacity-close-to-all-time-highs-willis/.

[543] Sclafane, Susanne. "Terror Risk Bond Market Unlikely, Says Swiss Re Americas CEO." Carrier Management, September 19, 2013. Accessed January 8, 2014. http://www.carriermanagement.com/news/2013/09/19/113254.htm.

[544] Ibid.

[545] GAO. *Terrorism Insurance: Status of Coverage Availability for Attacks Involving Nuclear, Biological, Chemical, or Radiological Weapons*. December 2008. Accessed December 10, 2013. http://www.gao.gov/assets/290/284287.pdf.

[546] Risk and Insurance Management Society, Inc. (RIMS). "President's Working Group on Financial Markets: Terrorism Risk Insurance Analysis." Letter to the Federal Insurance Office. September 16, 2013. Accessed December 5, 2013. http://www.rims.org/externalaffairs/PositionStatements/FederalIssues/Documents/RIMS%20TRIA%20Comments%20to%20PWG%202013.pdf.

[547] See, for example, Marsh & McLennan Companies, Inc. "Marsh & McLennan Companies Urges Lawmakers to Reauthorize Terrorism Risk Insurance Act During U.S. House of Representatives Hearing." News from Marsh & McLennan Companies. News. Last modified September 19, 2013. Accessed December 4, 2013. http://irnews.mmc.com/phoenix.zhtml?c=113872&p=irol-newsArticle&ID=1856356&highlight; Stephani, Justin. "All Testifying Members at Congressional Hearing Support TRIA Renewal." Insurance Networking News Breaking News, November 13, 2013. Accessed November 30, 2013. http://www.insurancenetworking.com/news/all-testifying-members-support-tria-renewal-congressional-hearing-33379-1.html.

[548] Author interview with industry executives.

[549] *State Insurance Regulation*: *History, Purpose and Structur*e. Kansas City: National Association of Insurance Commissioners. Accessed January 10, 2014. http://www.naic.org/documents/consumer_state_reg_brief.pdf.

[550] To understand insurance industry financials, see Insurance Information Institute (III). "2013 - First Nine Months Results." Last modified December 23, 2013. Accessed January 6, 2014. http://www.iii.org/articles/2013-first-nine-months-results.html.

[551] McMahon, Chris. "The New Data-Driven Insurer." Insurance Networking News (INN), September 1, 2013. Accessed November 30, 2014. http://www.insurancenetworking.com/issues/2008_98/data-driven-decision-making-32919-1.html.

[552] According to Gartner, big data is information of extreme size, diversity and complexity.

[553] Gartner. "Big Data." Accessed January 6, 2014. http://www.gartner.com/technology/topics/big-data.jsp.

[554] Towers Watson. "Property & Casualty Insurers Reveal Progress With Predictive Modeling Implementation in Towers Watson Survey." Last modified January 29, 2013. Accessed January 7, 2014. http://www.towerswatson.com/en-US/Press/2013/01/PC-Insurers-Reveal-Progress-With-Predictive-Modeling-Implementation-in-Towers-Watson-Survey.

[555] DHS. National Protection and Programs Directorate. *Cyber Risk Culture Roundtable Readout Report.* May 2013. Accessed December 20, 2013. http://www.dhs.gov/sites/default/files/publications/cyber-risk-culture-roundtable-readout_0.pdf.

[556] DHS. National Protection and Programs Directorate. *Cybersecurity Insurance Workshop Readout Report.* November 2012. Accessed December 20, 2013. http://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf.

[557] Ibid., 36.

[558] American Association of Insurance Services, Inc. (AAIS). "About AAIS." Home. Accessed January 7, 2014. http://www.aaisonline.com/Home.aspx.

[559] AAIS. "AAIS Launches Underwriting Platform for Commercial Output Program." Last modified December 11, 2013. Accessed January 8, 2014. http://www.aaisonline.com/AAISFrame/ConnectFrame/PressReleasesFrame/tabid/165/ArticleID/728/AAIS-Launches-Underwriting-Platform-for-Commercial-Output-Program.aspx.

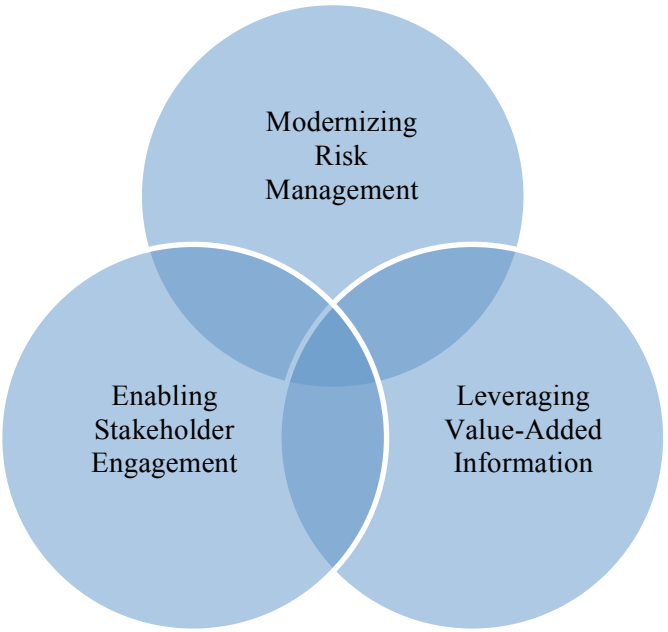
Pragmatic Solutions

It is difficult to precisely assess the effectiveness of traditional countermeasures — particularly strategic trade controls and sanctions regimes — in mitigating the risks rooted in global trade networks. However, the ongoing prevalence of drug trafficking and human smuggling testify to continued gaps, as does the constant stream of export and sanctions violation cases being pursued in the US, as elsewhere.[560]

As these cases make plain, security in an era of global value chains will not come through the efforts of governments alone. Traditional regulatory tools are overextended, and they already have run up against substantial jurisdictional and sovereignty limitations.

Many challenges can be better addressed by varying degrees of government cooperation with the private sector, NGOs, research institutions and the public, creating partnerships based on an understanding of which stakeholder is best suited for a particular task. By facilitating appropriate stakeholder engagement, government can help all involved to share information that will add value to each stakeholder's interests and allow for better risk management. This was the basic logic behind the three "strategic prerequisites" that the Partners in Prevention Task Force identified for sustainable public-private partnerships to combat nuclear proliferation and other transnational trafficking crimes.

Optimal Steps Toward 21st-Century Partnerships



Below, we elaborate on these three interrelated themes and recap the Task Force recommendations.

THE TASK FORCE RECOMMENDATIONS, REVISITED

Released in May 2014, the final report of the Partners in Prevention Task Force features seven targeted recommendations for modernizing public-private cooperation to advance both US security and economic competitiveness. While the Task Force report did not number the proposals, we do so below for ease of reference. The numbers do not represent priority order.

1. **Reward exporters whose internal compliance programs qualify them as "trusted traders."**
   The Commerce Department should pilot a voluntary regime that rewards "compliance-plus" practices in companies' internal export compliance programs. Benchmarks for the regime should be established with the assistance of a cross-sector industry group of export compliance professionals.

2. **Offer new benefits to logistics providers that take on greater export compliance burdens.**
   CBP and logistics service providers (LSPs) should co-create a voluntary program in which high-performing LSPs receive concrete benefits when opting to assume certain aspects of an exporter's compliance burden. The Border Interagency Executive Council should ensure strong interagency participation in this process.

3. **Develop a more streamlined information-sharing toolkit for trade and technology issues.**
   The Commerce Department and major trade associations should jointly develop a framework of technical and procedural options for two-way information sharing on issues related to trade, innovation and technology transfer. Industry peers should share best practices in protecting against illicit transshipment and other misappropriations of sensitive technologies.

4. **Promote layered port security through the SAFETY Act and Resilience STAR program.**
   DHS should consider Block Designation of SAFETY Act protections for private sector leaders in standards development related to trade/compliance processes. DHS also should expand the Resilience STAR Program to the transportation sector. Risk management experts and standards development bodies should support the current effort sponsored by the Department of Transportation's Maritime Administration to develop a Port Investment Toolkit.

5. **Develop a public-private "playbook" for resilient trade flows.**
   FEMA should issue clear guidance on public/private roles and responsibilities in restoring trade flows after both natural and man-made emergencies. Insurance providers, maritime industry stakeholders and standards development organizations should explore the viability of insurance and risk management products benchmarked against certified competency in business continuity planning and operations.

6. **Extend TRIA for five years and consider future changes to the program.**
   Congress should extend the Terrorism Risk Insurance Act (TRIA) for five years and establish a task force to report on possible program changes within 18 months. The private sector and broader public should help the task force identify other ways that market-based incentives might be introduced into the TRIA regime to enhance national security and promote development of the private market.

7. **Fully implement the International Trade Data System and leverage the BIEC more broadly.**
   The White House should closely monitor implementation of Executive Order 13659 (Feb. 2014), paying special attention to the broader mandate for the Border Interagency Executive Council (BIEC) to engage industry and other stakeholders to modernize trade facilitation and enforcement processes.

FORGING A NEW PARADIGM: FIVE IMPERATIVES

This report has noted many private-public efforts that could be further leveraged to enhance national security. A genuine partnership must begin by clearly identifying each stakeholder's interests, relative influence and capabilities. Stakeholders are then much better positioned to articulate the concrete objectives of their joint efforts and the most suitable engagement mechanism to pursue those ends. Below, we offer some broader examples of ways government and industry can jointly promote national and international security while also advancing their other vital interests. These examples complement the recommendations issued by the Partners in Prevention Task Force.

BROADEN HOW NATIONAL SECURITY IS DEFINED

In the context of global trade and economic activity, threats to the nation's security generally have been considered too narrowly. Government engagement with the owners and operators of domestic critical infrastructure has been well established at many levels. But cross-cutting issues such as supply chain security have not been adequately addressed. For example, it took a presidential directive for cybersecurity to be addressed more adequately within the context of critical infrastructure resilience. And although the National Strategy for Global Supply Chain Security has spurred considerable progress, its implementation to date has not given sufficient attention to US exports, focusing almost exclusively on import-related risks. [561]

Exports pose direct risks. Relevant threats to domestic critical infrastructure have not been sufficiently considered. Trading partner vulnerabilities affect us in the form of downstream re-imports of goods and services, as well as risks of technology diversion. Non-compliance with export controls and sanctions further opens the door to proliferation of dual-use and defense goods, undermining US national security and economic competitiveness.

Adapt the CI model

- Supply chain security needs to be addressed both within and beyond the critical infrastructure engagement model

- The federally mandated Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) should build on lessons from standards organizations and others who already have examined relevant supply chain security issues

Focus on exports in the context of global value chains

- Given the networked world of trade, we must consider the risks inherent in outbound trade flows — to our own ports, to our trading partners and to US economic and security interests abroad

- To give appropriate attention to national security and foreign policy goals, consideration should be given to increasing the resources of the Export Enforcement Coordination Center (E2C2)

Identify Key Information Gaps and Shortfalls in Operational Capacities

Both industry and government have information and operational gaps that they could help each other fill. The fundamental question emerges of what kind of information should be shared in a timely manner to help both industry and government better manage risks. To that end, standards for identifying and differentiating risks are critical.

While data exchanges and reporting models are being standardized to make better use of some information, neither government nor industry is giving sufficient attention to developing new sources of information and new performance standards. For example, exporters and logistics service providers that receive suspicious business solicitations often have little incentive to share that information and no anonymous way to do so.

Other emerging corporate and national security include increased risk of intellectual property theft and proprietary technology, whether due to deliberate exploitation or other factors. Exporters and logistics service providers want mutually agreed ways to demonstrate "compliance-plus" due diligence measures to mitigate these risks. To that end, a number of stakeholders need to engage in more regular and robust discussions about designing incentives for compliance with agreed standards.

Develop pilot programs in selected areas to allow for better risk management

- Working with exporters in selected sectors, logistics service providers, and other countries in regional and multilateral settings, government can develop compliance standards to better segment risk and enable high-performing industry players to obtain faster licensing/border processing, reduce supply chain/compliance risks and achieve other market benefits (reputation, insurance, tax/fee incentives, etc.).

- As part of a compliance framework, government can look to jump start aspects of compliance, such as a rating system for end-user checks, and can provide more specific threat information on "red flags" — including assessments of port security and transshipment risks.

- Consideration should be given to developing ways to check the compliance of participants, such as having an independent third party perform assessments, and to evaluate the benefits of the programs.

Streamline Information Sharing and Further Develop New/Existing Models

Everyone — from government to companies to think tanks — calls for more mutually-beneficial information sharing. It's time for action.[562]

Over the past five years, some progress has indeed been made in selected programs, particularly related to terrorism information sharing and suspicious activity reporting.[563] However, as noted

above, broader national security risks need to be better addressed, such as IP theft, cyber intrusions, and suspicious export-related requests. Companies' valid hesitation to ask questions of or engage government also needs to be addressed as they fear being targeted themselves for further government review or time-consuming engagement. Companies are often reluctant to share information because the risks and expense of sharing often outweigh the benefits they receive from government.

The Program Manager for the Information Sharing Environment (PM-ISE) plays an important role. However, it has not been able to address some fundamental issues of concern to firms.

The 2013 update to the National Infrastructure Protection Plan (NIPP) does include this call to action:

> "Undertake a partnership-wide review of impediments to information sharing to support efforts to address those challenges and develop best practices. Analyze legal considerations, the classification or sensitive nature of certain information, laws and policies that govern information dissemination, and the need to build trust among partners."[564]

Yet this passage is buried deep within the report, underscoring its low priority status.

Some current programs, such as the Enhanced Cybersecurity Services initiative, have been received favorably by industry.[565] However, its reach is currently limited. Successfully implemented, however, NIPP recommendations could be applied to existing or entirely new industry-government information sharing efforts.

Expeditiously address information-sharing issues

- An appropriately empowered office within the Executive Office of the President or the Department of Justice should lead an interagency review to clarify the chief legal, organizational and competitive obstacles to information sharing. It could bring greater clarity, for example, to when Safe Harbor rules apply or when PCII designation be easily expanded to the sharing of other national security-relevant information.

- The office leading the review should also offer guidelines for information sharing via independent third parties or anonymized reporting

- A third-party mechanism for anonymously querying government agencies on export-related questions should be piloted

- Further build on the Enhanced Cybersecurity Services initiative so that more types of firms can participate

Bring in Key Stakeholders Who Can Help Reduce Risk

The insurance industry has vast information on loss records in multiple areas. To date, however, it only has had the incentive to compile and share that information through associations post hoc[566] or in connection to specific parts of an individual company's business.[567] When

government can promote standards that reduce possible losses, the availability and terms of insurance products can be affected. The new Cybersecurity Framework is already having some effect, with insurers better able to "streamline" assessments.[568]

More collaborative research on standards would provide a better understanding of risks and result in more targeted insurance pricing and availability. The Treasury Department's Federal Advisory Committee on Insurance offers a vehicle for marshaling support from diverse stakeholders, as its members range from insurance commissioners to insurance industry representatives to researchers.[569]

Partner with the insurance industry

- Government should more systematically engage the insurance industry on broad security issues with the Treasury Department's Federal Insurance Office expanding to be the program manager of this engagement effort, and including all relevant stakeholders in discussions

- DHS Science & Technology should seed-fund industry collaboration on research related to losses of national security interest. What aspects of the new Cybersecurity Framework, for instance, are most important to reducing industry losses and producing security gains?

- FIO should be part of pilot projects on possible regulatory compliance standards and the possible generation of related insurance products and benefits

The private sector engages with government through various programs and is often confused about what's available and how best to get information. In addition, in critical infrastructure, industry outreach has occurred largely through major trade associations and Fortune 500 companies and has left smaller companies less engaged. Meanwhile, it is the smaller companies, wholesalers and distributors that account for the bulk of economic activity. C-TPAT often is cited as a model for industry-government partnership in the supply chain realm, but it faces considerable challenges in delivering concrete benefits to high-performing companies.

Complementing government-industry efforts with outreach to the broader public in targeted functional areas also deserves serious consideration. The public itself can play a role in ensuring national security — from whistleblower laws and incentives (as in IRS programs) to simple reporting and monitoring.[570] These steps must be sufficiently targeted to ensure government does not get diverted to investigating many false reports.

Bring new players into the mix

- Expand private sector outreach. The DHS Private Sector Office mission needs to be rethought. It currently is a catch-all for programs others do not address. Could it be re-structured or another office tasked to be a program management office for DHS and other government agencies' security programs, such as the FBI's, so that industry has more of a one-stop shop for security assistance and information sharing, including export concerns?

- Expand the private sector's "in-reach" to government. Could the Small Business Administration's tools to enhance businesses access to government data be better linked to US Export Assistance Centers and other government initiatives? There is potential not

only to expand small business exports but also increase industry participation in various areas of national security concern, from resilience planning to suspicious activity reporting.

- Engage the broader public in national security. [571] Consider using more targeted social media to promote reporting for suspected wrongdoing and a rewards program for the public and for company insiders to report on suspicious activities.

PROVIDE MORE TARGETED INCENTIVES

Terrorism risks cannot be well modeled. The insurance industry needs the support of the public sector if it is to be involved in underwriting these risks. Thus Congress passed the Terrorism Risk Insurance Act (TRIA), allowing government to provide reinsurance to the industry. The benefits of having the insurance industry involved are numerous: developments in high-risk areas are not stymied and effectively held hostage to terrorist threats; insurers can serve as "first financial responders" after an event and help share the cost burdens related to response and rebuilding; and in due course, security risks will be better reflected in underwriting models, ultimately helping insured parties to be less vulnerable and more resilient.

The insurance industry hesitates to cover a large number of risks, from radiological to chemical threats, and excludes homeowner coverage from terrorism risk coverage. Yet various risks that homeowners face, from earthquakes to floods to hurricanes, do have government backstopping in different forms. And other countries have different approaches to catastrophic insurance coverage for industry and consumers.

- Consider ways that catastrophic insurance can best be provided and whether certain standards could help better differentiate risks
- The Treasury Department's Federal Insurance Office should undertake a broad study of the costs and benefits of alternative approaches to government incentives for underwriting catastrophic risks
- The study should develop and consider the merits of alternative frameworks for better risk differentiation and/or pooling to support security interests and insurers' needs

Another domain in which targeted incentives could likely be employed to good effect is radioisotope production. Medical isotopes are widely used internationally and are made using enriched uranium, some even using highly enriched uranium that is dangerous for proliferation. Countries like Iran use medical necessity as a reason to seek enrichment capability. The development of alternative ways to provide the useful medical isotopes would decrease proliferation potential and eliminate one reason countries may develop dangerous uranium enrichment facilities as well as nuclear research reactors. To further global nuclear security, the US government needs to create incentives for private sector development of non-fission-produced medical radioisotopes.

- Jump-start new approaches to medical radioisotope production
    - Convene a White House-led interagency group. The Office of Science and Technology Policy, the National Security Council, or both entities acting jointly should bring together disparate agencies around a common purpose to curb the

nonproliferation threat posed by fission-sourced radiopharmaceuticals. Key actors would be the President's Science and Technology Adviser and the NSC Senior Director for WMD Terrorism & Threat Reduction.

- Provide appropriate regulatory relief and incentives. The Food and Drug Administration should consider relaxing restrictions on the development and testing of non-fission medical radioisotopes in the of non-fission medical radioisotopes. The Centers for Medicare and Medicaid Services might also expand measures already in place to discourage the use of HEU medical isotopes and to encourage use of non-fission isotopes.

- Support related research
  - Congress and the Executive Branch should continue and intensify support of basic scientific research in the DoE and elsewhere on new, non-fission medical radioisotopes. DoE should partner with the Canadian government, given the latter's efforts in this area.
  - Professional societies concerned with nuclear medicine research and treatment, such as the Society of Nuclear Medicine and Molecular Imaging, can support targeted study and internal discussion on the merits and use of non-enriched-uranium (NEU) isotopes in health care in dialogue with the national security community. Industry should also review what nongovernmental regulations, such as industry-wide standards, might be put in place to promote work in this area, and engage with government, to review the incentives and obstacles to developing NEU radioisotopes for medical treatment and bringing them to market on a large scale.

---

[560] DHS. Immigration and Customs Enforcement (ICE). "Fact Sheet: Counter-Proliferation Investigations." Counter-Proliferations Investigations. National Security. Fact Sheets. Newsroom. Last modified March 29, 2013. Accessed August 14, 2014. http://www.ice.gov/news/library/factsheets/counter-proliferations.htm.

[561] White House. *National Strategy for Global Supply Chain Security Implementation Update*. January 2013. Accessed August 14, 2014. http://www.whitehouse.gov/sites/default/files/docs/national_strategy_for_global_supply_chain_security_implementation_update_public_version_final2-26-131.pdf.

[562] See, e.g., US Congress. Senate. Testimony of Stephen L. Caldwell and Gregory C. Wilshusen on Critical Infrastructure Protection. *Observations on Key Factors in DHS's Implementation of Its Partnership Approach*: Hearing before the Committee on Homeland Security and Governmental Affairs. 113th Cong., 2nd sess., March 26, 2014. Accessed August 14, 2014. http://www.gao.gov/products/GAO-14-464T.

[563] See: US Information Sharing Environment (ISE). "ISE Business Model." What is ISE? About ISE. http://www.ise.gov/ise-business-model#transitions; GAO. *Information Sharing: Additional Actions*

Could Help Ensure That Efforts to Share Terrorism-Related Suspicious Activity Reports Are Effective. March 2014. Accessed August 14, 2014. http://www.gao.gov/assets/660/652995.pdf.

[564] DHS. *NIPP 2013*, 24. Accessed August 14, 2014. http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.

[565] DHS. "Enhanced Cybersecurity Services." Last modified March 10, 2014. Accessed August 14, 2014. http://www.dhs.gov/enhanced-cybersecurity-services.

[566] Insurance Institute for Business & Home Safety. "FORTIFIED Overview." Accessed August 14, 2014. https://www.disastersafety.org/fortified-main/.

[567] Verisk Analytics. "ISO Launches ISO Rapid Valuator for Excess and Surplus Insurance Markets." Last modified April 16, 2014. Accessed August 14, 2014. http://www.verisk.com/Press-Releases/2014/iso-launches-iso-rapid-valuator-for-excess-and-surplus-insurance-markets.html.

[568] Jackson, William. "Cyber Security Insurance Market." Information Week, April 21, 2014. Accessed August 14, 2014. http://www.informationweek.com/government/cybersecurity/cyber-security-insurance-market/d/d-id/1204578.

[569] US Treasury. "FACI Members." Offices. Organizational Structure. About. Last modified June 12, 2013. Accessed January 10, 2014. http://www.treasury.gov/about/organizational-structure/offices/Pages/faci_members.aspx.

[570] Decker, Debra. "Government Can't Do It All, But the Public Can Help." Government Executive, January 14, 2014. Accessed August 14, 2014. http://www.govexec.com/excellence/promising-practices/2014/01/government-cant-do-it-all-public-can-help/76832/.

[571] Office of Management and Budget. "Small Business Administration." Accessed August 14, 2014. http://goals.performance.gov/agency/sba.

Conclusion

We close by recalling part of the key takeaways from the May 2014 report of the Partners in Prevention Task Force:

> Globalization of trade and commerce has changed the nature of governance itself. Top-down regulatory and enforcement tools cannot keep pace with contemporary technological change or with the speed and volume of global freight movement. Achieving genuine security amid a range of complex cross-border threats requires new partners and new models for engaging those partners. Perhaps most important, it requires a deep and diverse set of industry partnerships.

Translating this strategic imperative into concrete actions — and further still, into sustainable progress — will be a challenging endeavor for many years to come. The seven task force recommendations, along with ideas in this report, highlight good places to start. By extension, they also serve as an invitation to government and industry stakeholders to further advance these critical efforts without delay.

Appendix:
Select USG Trade Security Initiatives

ACAS: Air Cargo Advance Screening Pilot	
Lead Agency	Transportation Security Administration, Department of Homeland Security
Purpose	A voluntary pilot program in which participants submit information pursuant to 19 CFR 122.48 at the earliest point possible prior to cargo being loaded onto aircraft bound for the United States. By participating in the program and submitting information participants can better aid the US identify and concentrate on high-risk cargo.
US Export/Import Focus	US imports
Notes	*Participant Eligibility:* Association with import air-cargo supply chain (is not commodity specific) *Participant Benefits:* • Increased efficiency for inbound cargo • Reduced paper processes *Information required for submission:* • Consignee Name and Address • Cargo Description • Total quantity based on the smallest external packing unit • Total weight of cargo • Air Waybill Number (Master Air Waybill)

ACE: Automated Commercial Environment

Lead Agency	Customs and Border Protection, Department of Homeland Security
Purpose	Streamlines export/import processing using the International Trade Data System to collect and distribute information required by federal agencies with trade-related responsibilities.
US Export/Import Focus	US exports and US imports
Notes	*Participant Benefits:* • Reduced border processing — electronic truck manifest • Ability to view shipment status and store data via the ACE Secure Data Portal • Industry representatives believe that clearance process should be much faster and more accurate • There will be mandatory use of ACE for all electronic manifest filing by December 2016, for all modes of transportation.

Advance Manifest Rules

Lead Agency	Customs and Border Protection (CBP), Department of Homeland Security
Purpose	Requires carriers and non-vessel operating common carriers (NVOCCs) to provide information on incoming cargo to the US CBP via electronic data interchange system. This allows CBP to identify potentially high-risk cargo. Transmission requirements depend on the mode of transportation: *Ocean Vessel:* o Non-bulk shipments: 24 hours before lading o Bulk shipments: 24 hours before arrival *Air:* o From NAFTA: 4 hours before "wheels up" o From Central and S. America: 4 hours before "wheels up" *Rail:* o Two hours before arrival in US *Truck:* o For FAST Participants: 30 minutes before arrival in US o For non-FAST Participants: 1 hour before arrival in the US
US Export/Import Focus	US imports
Notes	*Concerns:* Need more specificity on descriptions of cargo in order for CBP to quickly identify anomalies.

AEI: Advance Export Information Pilot

Lead Agency	Department of Commerce
Purpose	Evaluates a new data filing option in AES that "helps determine whether the advanced export information permits Customs and Border Protection to effectively screen exports and helps identify and mitigate risk with the least impact practicable on trade operations."
US Export/Import Focus	US exports
Notes	*Participant Eligibility:* Participants must: • Be a United States Party in Interest (which is the party that receives the primary benefit from the export transaction, be that manufacturer or wholesaler) • Have 12 months of export reporting history • Report a minimum of 10-shipments per month • Show compliance for export reporting • Be compliant with all federal regulations concerning import and export transactions *Participant Benefits:* Provides participants technical, operational and policy guidance

Blue Lantern

Lead Agency	Department of State
Purpose	Responsible for pre- and post-delivery checks of export items licensed by the Department of State, working with embassies to conduct post-delivery end-user checks.
US Export/Import Focus	US exports
Notes	US government concern with gaps in post-delivery checks — in 10 of 13 investigated cases, Blue Lantern Officers conducted post-delivery checks without visiting end users.

CCSP: Certified Cargo Screening Program

Lead Agency	Transportation Security Administration, Department of Homeland Security
Purpose	Designates facilities that can screen known shipper cargo (see Known Shipper Program).
US Export/Import Focus	N/A
Notes	100% of cargo transported on a domestic passenger aircraft must be screened *Participant Eligibility:* • Application • Onsite assessment of facility to become Certified Cargo Screening Facility (CCSF) • Company must ensure employment of secure chain custody methods throughout supply chain *Participant Benefits:* • Allows company to perform piece-level cargo screening at the facility, prior to the cargo arriving at the air carrier to ensure that configurations are not broken down at airport. • Easy to acquire certification if already part of C-TPAT. *Difficult to expand to international inbound cargo.*

CSI: Container Security Initiative

Lead Agency	Customs and Border Protection (CBP), Department of Homeland Security
Purpose	Aims to security at international ports that import into the United States, the Initiative seeks to increase international ports' ability to use automated targeting tools to identify suspicious containers — including utilizing X-ray and gamma ray machines and radiation detection devices.
US Export/Import Focus	US imports
Notes	As of May 2011, 58 ports were part of CSI. *Participant Benefits*: • Technology training for host customs administrations • Intelligence exchange with host customs administrations. *Concerns:* • Technology being provided is not adequate to actually detect threats (including gamma-ray and radiation devices). • Incomplete documents could result in customs agents not knowing what to look for. • Need for expansion and more funding. However it is difficult to expand program due to sovereignty logistics make it difficult to open new ports. • Difficult to modify program to allocate resources more effectively: ending program in port often offends host government. • CBP has not adequately assessed ports for risks to cargo.

C-TPAT: Customs-Trade Partnership Against Terrorism

Lead Agency	Customs and Border Protection, Department of Homeland Security
Purpose	Certified industry partners sign an agreement to implement specific security measures and best-practices across their entire supply chain.
US Export/Import Focus	US imports
Notes	*Participant Eligibility:* There are two levels to C-TPAT: certification (Tier 1) and validation (Tier II) • Tier 1: online application • Tier 2: Follow up on-site inspection by Supply Chain Security Specialist (SCSS) *Participant Benefits:* Companies that are validated as C-TPAT are considered low risk by the government, and are provided with: • Mitigation of importer security filing liquidated damages claims • Fewer cargo exams • Expedited clearances • Enhanced regulatory risk profile As of November 2013, there were 10,675 C-TPAT certified partners Among exporters, there was a 70 percent approval of expanding C-TPAT for exporters *Concerns:* • Industry often voices objections to the premise of C-TPAT, arguing it has become a de facto requirement for companies to do business with other companies. • Government remains concerned about processes used to validate that C-TPAT members meet security criteria.

DSS: Defense Security Service

Lead Agency	Department of Defense
Purpose	Oversees the export of classified materials out of the United States and provides foreign ownership and control countermeasures to ensure proper end-use and prevent retransfer. All shipments of classified materials must be transported by a carrier who holds a DSS facility clearance.
US Export/Import Focus	US exports
Notes	There are currently 13,500 DSS cleared contractor facilities. *Participant Eligibility:* DSS Cleared Carriers work with a DSS Industrial Security Representative to establish a proper industrial security program. *Participant Benefits:* Ability to process and ship classified materials.

FAAP: Foreign Airport Assessment Program

Lead Agency	Transportation Security Administration, Department of Homeland Security
Purpose	Conducts security assessments and provides assistance and technology to foreign airports (passenger and all-cargo) that are the last stop for imports into the United States.
US Export/Import Focus	US imports
Notes	Program currently includes 300 foreign airports *Participant Eligibility:* Categorizes airports based on three tiers of risk to determine depth and frequency of investigations. *Participant Benefits:* US government technology and training to those foreign airports that are not up to the necessary standard. *Concerns:* • US-provided assistance and technology is not always effective. • Foreign airports lack the ability to implement, use and maintain technology.

FAST: Free and Secure Trade

Lead Agency	Customs and Border Protection (CBP), Department of Homeland Security
Purpose	Increases efficiency of trucking trade within North America (between Canada and Mexico) through pre-screening and validation of supply chain actors.
US Export/Import Focus	US exports and US imports
Notes	There are currently around 78,000 commercial drivers certified under FAST. *Participant Eligibility:* Online application — must prove that every link within the supply chain is C-TPAT certified (carrier, importer, and manufacturer). *Participant Benefits:* • Access to fast lanes at border crossings • Reduced number of inspections • Shorter time period for sending e-manifests (30 minutes before arrival for FAST members, 1 hour before for non-FAST members) • Front-of-the-line processing for CBP inspections. *Concerns:* • Trouble with implementation including the ability for truckers to access FAST lanes in Mexico. • Vetting process — trusted shippers are being caught smuggling. • US Government sees a need for expansion of the program, but must ensure that the benefits (such as FAST lanes) can be used efficiently. • Still unclear whether FAST lanes are providing reduced wait times.

Golden Sentry	
Lead Agency	Defense Security Cooperation Agency, Department of Defense
Purpose	Monitors end use of US origin government-to-government sold or leased defense exports in order to prevent misuse or unauthorized transfer to items.
US Export/Import Focus	US exports
Notes	Golden Sentry is maintained by the Combatant Commands, US Diplomatic Missions, Defense Threat Reduction Agency and the Defense Institute of Security Assistance Management.

IPSP: International Port Security Program	
Lead Agency	United States Coast Guard, Department of Homeland Security
Purpose	Arranges reciprocal visits and education programs with officials at foreign ports. Provides technical assistance to strengthen security at foreign ports that export to the US.
US Export/Import Focus	US imports
Notes	As of June 2013, 151 countries were included in IPSP. *Participant Benefits:* Training and education seminars.

Known Shipper Program	
Lead Agency	Transportation Security Administration, Department of Homeland Security
Purpose	In order to submit to a direct air carrier, each indirect air-carrier (air freight forwarder) must have a known shipper program which evaluates the shipper's integrity and validity.
US Export/Import Focus	N/A
Notes	Required for all indirect air-carriers shipping on domestic passenger flights. TSA inspections to ensure that shippers comply with requirements. *Participant Eligibility:* • Submit shipper data to US government Known Shipper Management System. • Certification process involves a scoring system based on congruence with outside sources. *Participant Benefits:* Only known shippers can ship cargo on domestic passenger aircraft. *Concerns:* • No longer cost effective to maintain Indirect Air Carrier Certification. • Fear of falsification of documents, especially with increasing applications. • Need for improved inspections.

Megaports Initiative	
Lead Agency	National Nuclear Security Administration, Department of Energy
Purpose	Works to equip and train foreign port operators with radiation detection technology to scan container traffic regardless of destination.
US Export/Import Focus	US imports
Notes	As of August 2012, 48 ports were involved in the Megaports Initiative *Participant Benefits:* Assistance with installation of radiological detection equipment. *Concerns:* • Need for the US to develop radiological scanning in partner countries, since no other countries are providing this aid. • US government has decided to halt expansion of program with budget cuts, given that most of the high-profile ports have been covered.

NMMSS: Nuclear Materials Management and Safeguards System	
Lead Agency	Nuclear Regulatory Commission, Department of Energy
Purpose	A reporting system to track nuclear materials: • Within the US • Imported into the United States • Exported abroad • Foreign obligated nuclear material currently in the US • US government owned nuclear materials Also provides oversight of nuclear facilities by providing information to the IAEA.
US Export/Import Focus	US imports and exports
Notes	NMMSS data is not exhaustive. It reflects the best available information on US exports and retransfers.

Project Guardian

Lead Agency	Bureau of Industry and Security (BIS), Department of Commerce
Purpose	Aims at liaising with and increasing outreach to US companies that produce dual-use goods in order to provide training on identifying suspicious customers and encourages cooperation in with BIS on risky end-users.
US Export/Import Focus	US exports
Notes	In FY13, BIS initiated 78 outreach contacts. There has been an overall increase in outreach contacts under Project Guardian since FY06. *Participant Eligibility:* Producers of dual-use goods under EAR. *Participant Benefits:* Government training on risk identification.

Project Shield America

Lead Agency	US Immigration and Customs Enforcement (ICE), Department of Homeland Security
Purpose	Reaches out to producers of sensitive munitions and strategic technology to mitigate proliferation to terrorists or other questionable end-users. Four-pronged approach: • Inspection and interdiction of illegal shipments at outbound ports • Investigations into illegal shipments based on risk factors • Industry outreach by increasing training on export controls and suspicious activity reporting, and soliciting cooperation in identifying risky end-users • International cooperation with foreign governments to identify risks and support investigations.
US Export/Import Focus	US exports
Notes	*Participant Eligibility:* All companies exporting sensitive munitions and strategic technology are eligible for Project Shield outreach. In general, ICE determines outreach via publically available information and government export data. *Participant Benefits:* Government training on risk identification and export controls.

Secure Freight Initiative	
Lead Agency	Customs and Border Protection, Department of Homeland Security
Purpose	Tests feasibility of 100 percent screening in certain ports to increase detection of containers transporting nuclear and radiological materials in foreign ports.
US Export/Import Focus	US imports
Notes	*Concerns:* • Inability for required ports to meet 100 percent screening requirements and ensure efficiency • Technology is not ready to ensure 100 percent screening and efficiency. • Originally the program was active at six international ports, including in Pakistan, Honduras, the United Kingdom, Oman, Singapore and Korea. As of 2012, only the Port of Qasim in Pakistan is participating. However, the other ports are active in the CSI.

Sentinel	
Lead Agency	Bureau of Industry and Security, Department of Commerce
Purpose	Responsible for pre- and post-delivery checks of export items licensed by Commerce Department (includes dual-use nuclear items), working with embassies to conduct post-delivery end-user checks.
US Export/Import Focus	US exports
Notes	*Concerns:* • There is a need for increased end-use checks • With upcoming export reforms and changes, Commerce has not assessed whether it will be able to conduct increased end-use monitoring.

SSCP: Secure Supply Chain Pilot Program

Lead Agency	Food and Drug Administration (FDA), Department of Health and Human Services
Purpose	Allows for expedited import of select drugs for pre-cleared companies to allow CBP and FDA to concentrate on high-level threats. Creates incentives for industry to abide by best practices.
US Export/Import Focus	US imports
Notes	*Participant Eligibility:* • Comply with FDA requirements • Operate a C-TPAT certified secure supply chain • Outlined plan to quickly rectify any FDA identified problems with a specific import • Effective recall plan in place. *As of February 2014, 13 companies were participating, but up to 100 companies eligible to participate in pilot.* *Participant Benefits:* • Expedited import of select drugs. • Company maintains control of drugs from production abroad through entry into the US.

TWIC: Transportation Worker Identification Credential	
Lead Agency	Transportation Security Administration (TSA), Department of Homeland Security
Purpose	Vets maritime workers who apply for unescorted access to authorized areas of ports and vessels that fall under the Maritime Transportation Security Act of 2002.
US Export/Import Focus	N/A
Notes	*Participant Eligibility:* Undergo a security threat assessment (background check). Currently, around 2,534,774 individuals hold a TWIC card. *Participant Benefits:* Access to TSA restricted areas. *Concerns:* Assessments of program were flawed, and thus it is difficult to determine the effectiveness of the program in improving port security.

VEU: Authorization Validated End-User

Lead Agency	Bureau of Industry and Security, Department of Commerce
Purpose	Maintains security while promoting industry competitiveness by allowing for export, re-export and transfer of eligible dual-use items to validated end-users in India and China.
US Export/Import Focus	US exports
Notes	*Participant Eligibility:* • Only end-users that have been approved, and thus are in compliance with requirements of VEU. • Export authorizations to VEUs consider the VEU's adherence to US export laws. • VEU only applies to companies in India and China • Agreement for onsite reviews Eligible items include semi-conductors, computer technology, software (excluding source code) specially designed for the development of equipment controlled by ECCN. Items obtained under authorization VEU may be used only for civil end-use and may not be re-exported. Exporters are required to submit annual reports on each end-user.

Acknowledgements

Above all, I wish to thank Brian Finlay, Stimson's managing director and the architect of the Partners in Prevention project. He not only enabled this initiative to come into being and thrive. He also gave me an incredible opportunity to do the kind of work I love to do, in a fun and supportive environment.

A major part of that environment was the project team at Stimson. Debra Decker, Shannon Dick, Alex Georgieff and Gerson Sher provided outstanding support from end to end. Their selflessness in advancing the work of the project while often remaining in the background was truly impressive. For valuable assistance with research, writing, and editing tasks, I also thank Devon Blount, Alex Davis, Wes Dravenstadt, Sydney Fields, Natasha John, Jessica Kosmider, James McKeon, Apurva Pande and Christy Wagner.

I would be remiss without again recognizing the crucial role played by the Partners in Prevention Task Force, led by Jay Cohen (RADM, USN, Ret) and Barry Blechman. The recommendations they issued earlier this year have rightly gained widespread praise from audiences in government and industry alike. Stimson is now leveraging that success to effect meaningful, tangible results.

In addition to the Task Force, our success would not have been possible without the participation of hundreds of private sector partners. While we are genuinely grateful to each of them, the following companies and associations deserve special recognition for being exceptionally generous with their time and insights.

Aerospace Industries Association (AIA)
American Association of Exporters and Importers (AAEI)
Boeing
Chertoff Group
Cisco
Covington and Burling
Express Association of America (EAA)
GE
IBM
Liberty Mutual
Maersk
National Association of Manufacturers (NAM)
National Customs Brokers & Forwarders Association of America (NCBFAA)
National Foreign Trade Council (NFTC)
NTELX
PricewaterhouseCoopers (PwC)
Rolls-Royce
US Chamber of Commerce
US Council for International Business (USCIB)
Venable LLP

Finally, for the financial support that made this work possible, sincere thanks go to Emma Belcher and the John D. and Catherine T. MacArthur Foundation; Carl Robichaud and the Carnegie Corporation of New York; and the Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction (PASCC), Center on Contemporary Conflict, Naval Postgraduate School.

Nate Olson
Project Manager

Making Public-Private Security Cooperation More Efficient, Effective and Sustainable

In May 2014, the Stimson Center's Partners in Prevention Task Force endorsed seven proposals to close security gaps in global trade by better leveraging market incentives. Directed mainly at US policy and industry audiences, the recommendations were the product of an 18-month collaboration with high-tech manufacturers and service providers, transport and logistics firms, and insurance providers.

This report is based principally on the varied research and analytical products prepared by Stimson project staff for the Task Force prior to May 2014. It parallels the Task Force proposals in its focus on exports as an area critical to contemporary global trade and security issues. While the Task Force recommendations were highly targeted and prescriptive, this report covers a much wider substantive range and elaborates key background issues. In so doing, it lays bare the urgent need to modernize public-private partnerships for a 21st-century economic and security environment.

Stimson enters 2015 well into the next phase of this work, building on the success of the Task Force proposals to ensure tangible, sustainable outcomes. To the many stakeholders in industry and government whose collaboration has allowed us to reach this point, we emphasize our sincere thanks – and our enthusiasm for what lies ahead.

STIMSON
www.stimson.org