Deloitte.

IDGA
Institute for Defense and Government Advancement

Cargo Security Summit 2014 Post-Summit Report: Securing the Global Supply Chain to Protect the American Consumer

"…it is only through ongoing debate, analysis, and collaboration that policy makers and industry leaders can hope to secure the American people while fostering an environment that remains conducive to the free movement of goods."

— Securing the Global Supply Chain to Protect the American Consumer

Notes from the moderator

"The 2nd IDGA Cargo Security Summit is an example of how stakeholders responsible for the movement of commercial cargo both domestically and internationally strive to secure the safety of their supply chain. Throughout the Summit, we discussed the need to create trade processes that are secure, consistent, and harmonized across operations so that commercial cargo stakeholders function in an environment defined by predictability, partnerships, and prosperity. We heard from key stakeholders on how they are developing systems and processes that reflect the operational realities of modern commerce and dynamic trade practices. This two day conference helped attendees deepen their understanding of the way business and industry continue to operate in the ever changing and challenging global cargo marketplace."

Bob Jacksta — Strategy & Operations, Deloitte Consulting, LPP

Bob Jacksta retired from U.S. Customs and Border Protection (CBP) after a 34 year career in federal law enforcement. During his career Mr. Jacksta demonstrated a deep knowledge of customs and immigration issues and a keen understanding of how technology can be applied to border security. As Deputy Assistant Commissioner for the Office of Field Operations, he managed border security and anti-terrorism efforts, international trade compliance, anti-smuggling, passenger operations, and oversight of the policies, programs and operations of 20 major field offices and 326 ports of entry. During his tenure at CBP, Mr. Jacksta served in a number of senior executive positions with responsibility for policies and programs in support of radiation detection and non-intrusive technology for supply chain security through the Customs-Trade Partnership Against Terrorism (C-TPAT), international security through the Container Security Initiative, National Passenger and Cargo Targeting Centers, and advanced passenger and trade information systems.

Contents

Introduction

In the nearly thirteen years since the September 11, 2001 terrorist attacks on New York City and Washington, D.C., the global security community's focus on preventing similar attacks has been unrelenting. Indeed, the United States (U.S.) has been free of large-scale terrorism since 2001 due in large part to these efforts. Despite this success, public discourse related to domestic and international terrorism is largely focused on the movement of individuals (i.e., the public transportation sector). While this emphasis is unsurprising given that attacks as early as the 1988 bombing of Pan Am Flight 103 were designed to inflict mass casualties on the traveling public, it must not result in an overly prescribed view of the terrorist threat landscape.

In fact, a critical—but often under discussed—element of this landscape involves not the movement of people, but of the goods and products essential to life and economic vitality. While ensuring the safety of the traveling public is a subject that draws our attention as citizens, the American people generally view movement of goods simply as consumers. Even major government initiatives designed to secure the cargo supply chain, such as the Implementing Recommendations of the 9/11 Act's 100% screening mandate, focus primarily on preventing use of cargo as a weapon against passengers and crew on commercial and cargo aircraft. This perception must change, as a breach in the cargo supply chain, particularly with regard to consumable goods such as pharmaceuticals, could prove catastrophic—resulting in substantial loss of life and revenue. This paper will explore the nature of this threat, how it can be mitigated, and the primary challenges that remain when attempting to secure a complex supply chain that moves nearly two trillion dollars' worth of goods annually.

This document draws extensively from the Second Annual Cargo Security Summit held in November 2013 by the Institute for Defense & Government Advancement (IDGA). These Summits bring together thought leaders from both the private and public sectors to discuss the challenges of securing the global supply chain and explore viable solutions for both the short and long term.

The cargo supply chain — A clear and present threat

The impacts of a breach in cargo security are consequential and far-reaching. Perhaps the most obvious vulnerability in the global cargo system is the possibility of terrorist attack. Terrorists have used air cargo as an attack delivery platform in the past, most recently in October 2010, when Al-Qaeda in the Arabian Peninsula shipped two explosive devices concealed in printer ink cartridges from Yemen on aircraft bound for the U.S. (Mullen, Case Study: The Air Cargo Advance Screening Project, 2013). The potential for significant loss of life stemming from this incident alone provides compelling motivation for a strong government response to prevent such attacks in the future. Unsurprisingly, the U.S. Department of Homeland Security (DHS), which was created in the aftermath of 9/11, has experienced significant budget increases since its inception, representing a 59% total increase between fiscal years 2003 and 2014 (DHS, 2014).

While the risk of terrorism (i.e., the intentional use of cargo to inflict major casualties) is undeniable, it is crucial that we not overlook the unintended loss of life that may stem from breaches in the cargo supply chain through cargo theft. Given that a single pharmaceutical shipment can range in value from several thousand to several million dollars, it is unsurprising that cargo is a favored target of thieves. While the financial implications of such a security breach are self-evident, pharmaceutical theft can also lead to serious injury and loss of life.

Consider the public health implications when pharmaceutical products are stolen, mishandled, and later re-enter the supply chain. Because drugs are consumable goods, factors such as temperature control are critical to preserving their integrity. Stolen pharmaceuticals are often mishandled along the supply chain, which poses serious risks to products reliant upon careful environmental control. This issue is further complicated and made more concerning given that drugs can now be counterfeited with relative ease. In fact, the World Health Organization (WHO) estimates that between five and eight percent of the worldwide pharmaceutical trade is counterfeit (Schuster). In light of this fact, it is not hard to imagine a scenario where hundreds of patients receive life-preserving medication that has been damaged or replaced with counterfeit product—resulting in large scale casualties. In the least nefarious scenario, a breach in supply chain

security may turn properly prescribed and consumed medications into unintended weapons of mass destruction. Even more alarming is the fact that intentional tampering of such products could serve as a compelling mode of terrorist attack.

Though obvious, the financial consequences of cargo theft must not be underestimated. In 2010, pharmaceutical giant Eli Lilly fell victim to an $80 million cargo theft from a Connecticut warehouse—the largest such heist in industry history (Applebome, 2012). The severity of this loss prompted Ely Lilly to publish a report on cargo security best practices for use by industry stakeholders, signifying that security issues transcend competition concerns. The fact that this financial loss resulted from a single theft illustrates the serious implications such activity could have for the U.S. economy. Indeed, between 2009 and 2010, American companies lost nearly $300 million dollars to cargo theft in the pharmaceutical sector alone (Efrati & Loftus, 2010). Internationally, financial losses stemming from cargo theft in São Paolo and Rio de Janeiro—two of the highest risk locations in terms of cargo theft—totaled $1 billion in 2012, though industry experts estimate this value is closer to $10 billion (Jones, 2013). Were these losses not enough, manufacturers also run the risk of lawsuits from injured consumers in addition to further financial loss stemming from a decline in sales, as was experienced by Johnson & Johnson in 1982 when seven people died after consuming cyanide-laced Extra Strength Tylenol (Associated Press, 2013). While this case remains unsolved, several theories are posited on a breach in chain of custody which allowed for introduction of the toxic medication at a warehouse facility (Bartz, 2012).

Cargo terrorists and thieves — Who are they?

To fully appreciate the nature of the threat posed to the cargo supply chain, one must understand the sources of these threats—namely terrorists and thieves. The former has received unprecedented attention in the post-9/11 world, with groups such as Al-Qaeda obtaining universal recognition. The term "terrorist" usually evokes images of foreign organizations—the threat coming from the proverbial "other"—a perception reinforced by images of Al-Qaeda operatives receiving paramilitary training in the distant mountains of Afghanistan.

However, as the Oklahoma City Bombing of 1995 demonstrated, terrorists can also come from closer to home. Insider threat is particularly concerning with regard to the cargo supply chain, given the number of individuals involved in the movement of goods from point of origin to final destination. Dozens of sorters, fork-lift operators, and drivers may come in contact with a single package in the course of its journey across the globe. In theory, each of these individuals could have the opportunity to tamper with a shipment, thereby breaching the chain of custody on which secure movement of goods depends. Given this potential for tampering, any discussion related to securing the cargo supply chain must consider insider threat. Indeed, in this environment, a disgruntled freight forwarding employee could prove as dangerous as any trained terrorist operative.

The nature of the threat posed by cargo thieves has also changed in recent decades. Gone are the somewhat primitive criminals who were able to infiltrate a warehouse and pilfer electronics with little more than bolt cutters and stealth. Today's successful cargo thieves are often highly sophisticated, well trained, and equipped with cutting-edge technologies. Indeed, the culprits in the $80 million Eli Lilly heist were equipped with tools to disable the corporation's advanced security system and leveraged industrial tractor-trailers and fork-lifts in the process (Applebome, 2012). Furthermore, far from being solitary actors, cargo thieves often work as part of larger syndicates with connections to crime across the world. In both Brazil and Mexico, cargo is often stolen and resold so that profits can be used to support the drug trade (Jones, 2013). Thus, just as the cargo supply chain lends itself to a particularly diverse set of potential terrorist actors, it is also exposed to theft at the hands of some of the world's most sophisticated criminals.

Mitigation strategies — Securing the global cargo supply chain

The complexity of the cargo supply chain, coupled with a diverse range of adversaries, necessitates an equally advanced response from national governments and corporations. To be sure, simply keeping shipments under lock and key is no longer enough. Instead, the global cargo supply chain increasingly depends upon a combination of time-tested logistics best practices and cutting-edge countermeasures.

Technology

Foremost among these advances are technological improvements, such as shipment tagging, advanced global positioning satellite (GPS) capabilities, and geo-fencing. Together, these advances exemplify the critical role of technology in securing cargo. Shipment tags, which often resemble barcodes, provide data crucial to effective decision making. These data can reveal systemic process errors, such as unsubstantiated fees, that could be indicative of cargo security breaches. In one example, shipment tagging helped a manufacturer realize that it was paying canal fees though its shipments were not actually crossing the canal in question. Thus, the manufacturer was better able to track the movement of its shipment, thereby preserving chain of custody and avoiding fraudulent fees (Radford, 2014).

Similarly, modern GPS systems allow for real-time monitoring of shipment location along pre-determined routes. Unlike GPS of the past, today's systems are more accurate, compact, and efficient. In fact, use of cellular towers as a means of triangulating a shipment's location provides readings that are considerably more consistent and accurate—sometimes pinpointing locations to within 100 feet (Forsaith, Pharmaceutical Supply Chain Security, 2014). In the past, GPS technology depended upon long-range satellites, which provided inaccurate readings and were often non-functional when shipments were in an enclosed space (e.g., garage, tunnel) (Forsaith, Pharmaceutical Supply Chain Security, 2014). In addition to enhanced accuracy, modern GPS systems are far smaller and leverage more efficient, long-life batteries. Taken together, these improvements dramatically enhance the effectiveness of GPS technology. It is now possible to monitor the movement of goods from point of departure to arrival, allowing for immediate identification and resolution of unauthorized route deviations. This unprecedented rapid response capacity is a crucial component to recovery of stolen goods.

While tracking cargo movement is a critical security element, so is maintaining chain of custody while a shipment is stationary. To this end, some shippers have instituted intelligent geo-fencing to ensure that shipments remain within pre-approved geographies/routes and are automatically secured when immobile for a pre-determined period of time. Prior to use of geo-fencing, drivers completed a substantial list of security protocols each time they stopped along their routes, even if just for a "quick pit-stop." These protocols—which included detaching/locking the trailer and activating air-cuff brakes—were laborious and unlikely to be fully implemented on brief stops, thereby leaving shipments exposed. However, geo-fencing verifies cargo locations at regular intervals, and will automatically lock shipments if immobilized for a pre-set period of time (e.g., 10 minutes). The driver must then contact shipping headquarters to unlock the shipment. Should no one make this call, shipping headquarters will receive an alert—prompting cargo recovery procedures and potential penalties for the driver (Cobb, 2013). Thus, technology increases driver accountability, while reducing the window during which shipments are unattended and vulnerable.

Data Sharing

While the benefits of technological advances are undeniable, improvements in the availability and use of cargo supply chain data have also improved security. As the supply chain becomes increasingly complex, the amount of data available has also grown. Thanks to technological advances—such as those discussed above—data are now accessible in near real-time. Improvements have also been made with regard to data sharing both within private shipping entities and between actors in the public and private sectors. There can be little doubt of the value Eli Lilly's cargo security best practices report provided to the global supply chain. This unprecedented example of intra-industry information sharing is critical to ensuring that major cargo actors remain at the forefront of supply chain security. Positive relationships and fluid dialogue between shipping companies and law enforcement have also proven highly valuable, resulting in more effective tracking of criminals and recovery of stolen goods (Forsaith, Mitigating Market Risks and Cargo Theft, 2013).

The importance of such relationships is reflected in the existence of the Pharmaceutical Cargo Security Coalition (PCSC), a national organization dedicated to preventing theft of in-transit pharmaceutical products by promoting strong ties with law enforcement. Purdue Pharma Technologies' Supply Chain Director and PCSC member, Charles Forsaith, explains that the group maintains strong ties with law enforcement by awarding agencies for successful shipment recovery, recognizing individuals who are particularly attentive to supply chain security, and contributing to law enforcement programs such as Drug Abuse Resistance Education (D.A.R.E.). In return, law enforcement agencies support PCSC's mission by making pharmaceutical recovery a priority.

The effectiveness of this mutual understanding was demonstrated when a narcotics shipment went missing in Atlanta, Georgia. Upon learning of the theft, PCSC leveraged pre-existing relationships to directly contact John Cannon, the head of the Georgia Bureau of Investigations' (GBI) Major Thefts Unit. Cannon mobilized his team at the GBI and was able to locate the shipment within hours (Forsaith, Pharmaceutical Supply Chain Security, 2014).

There can be no doubt that this remarkably rapid response was due in large part to sound working relationships between the pharmaceutical industry and local law enforcement.

Public-private coordination can also be attributed with helping governments address challenges associated with the dramatically increased cargo volumes that preclude resolving security threats at the point of import. Indeed, this collaboration permits threat resolution early in the supply chain and, ideally, before shipments reach national borders (Gina & Farrely, 2013).

A crucial first step to this "downstream" approach is identifying which shipments require close scrutiny (i.e., "high risk" cargo), and providing that additional attention as needed. To this end, the U.S. implemented a joint Customs and Border Protection (CBP) and Transportation Security Administration (TSA) Air Cargo Advanced Screening (ACAS) Pilot, which targets potentially high-risk air cargo shipments bound for the U.S. CBP and TSA launched the ACAS Pilot in response to the October 2010 Yemen incident. Fortunately, while the improvised explosive devices (IEDs) used in this instance were identified and neutralized, one had already flown three of four legs and, the other, two of three legs of its journey to U.S. airspace. In the aftermath of this incident, CBP and TSA determined that had certain critical information associated with

these shipments been gathered and vetted prior to their departure from Yemen, the cargo could have been stopped pre-flight. Thus, the ACAS Pilot was developed to serve as a mechanism for advanced analysis of such data associated with all shipments destined for the U.S. or routed to travel its airspace (Kennally, 2012).

The ACAS Pilot provides an example of information sharing between the public and private sectors to ensure supply chain integrity. Through the ACAS Pilot, the private sector provides shipment-level data to the government. At the same time, the government shares intelligence about certain shipments with private sector ACAS participants, as appropriate. This information sharing enables the U.S. Government to target cargo screening based on risk factors, a process known as advanced risk-based targeting—all before shipments reach American airspace (Mullen, Case Study: The Air Cargo Advance Screening Project, 2013).

Non-profit Innovation

While the ACAS Pilot is an excellent example of agency-driven collaboration between the public and private sectors, it is important to note that non-profit organizations can also be the impetus of progress in this area. In fact, governments, non-profits, and corporations can benefit from seemingly unrelated philanthropic efforts.

For example, Australian millionaire philanthropist, Andrew Forrest, and the non-profit organization Walk Free, leverage data analytics to track and monitor the global human trafficking supply chain. Developing an understanding of the human trafficking supply chain such that it can be disrupted is not unlike gathering insights to better secure the cargo supply chain. Walk Free published the Global Slavery Index, which uses data analytics to rank countries based on the estimated prevalence of slavery. This tool may lead to a policy change in the United Kingdom (U.K.), which would require companies to monitor and audit their supply chains for human trafficking (Parker, 2013). This audit framework could very well be

applied to analysis of the global cargo supply chain. Only by identifying and tracking key supply chain weaknesses can law enforcement and national security agencies hope to thwart cargo terrorists and thieves. Such opportunities for collaboration should be cultivated through regular interaction and communication between representatives of private industry, government agencies, and academic institutions. Given the increasing sophistication of actors with malintent, it is crucial that cargo security stakeholders leverage innovation to remain ahead of the curve—ensuring that they are well positioned to respond to the next mode of attack.

Looking to the future — Remaining cargo security challenges

While progress has been made in the realm of cargo security, challenges remain as the international community endeavors to secure an increasingly massive and complex global supply chain.

International Collaboration

To build upon progress made in moving cargo security to the earliest possible points of the supply chain, the U.S. must continue to develop strong relationships with customs officials and security agencies around the world. Given jurisdictional limitations and the complexity of global commerce, it is impossible for the U.S. Government to secure the supply chain without close collaboration with foreign partners. Failure to build sound working relationships has resulted in less than ideal results in the past. In 1991, U.S. copyrighters publically blamed Emirati law enforcement for a flourishing pirated video market in the Persian Gulf, which did little more than damage relationships with local officials. In light of this failed approach, the Motion Picture Association of America (MPAA) changed tack by sending copyrighters to Dubai to work with local officials to address the problem. Emirati authorities reacted positively, forming a relationship with a prominent law firm that addressed the issue through raids and other enforcement tactics (Chambers, 2013). This example demonstrates the need for international coordination if the U.S. hopes to secure a supply chain over which it has limited control. The U.S. must approach foreign governments as partners in this effort, addressing security issues in a collaborative and mutually beneficial fashion.

Standardized Systems

A critical first step to fostering international collaboration is standardization of cargo security systems. It is vital that the U.S. Government seek early alignment with international organizations, foreign governments, and other partners to develop internationally-recognized standards, procedures, and processes for all major cargo security initiatives (e.g., advanced shipping data collection for the ACAS Pilot). This effort may minimize system and requirement variability, thereby avoiding duplicative data submissions and risk-assessment, where possible. To this end, TSA developed the National Cargo Security Program (NCSP) to determine whether foreign air cargo screening programs provide a level of security commensurate with that of existing U.S. regulations. Partners that meet TSA screening requirements are recognized under NCSP and are permitted to screen U.S.-bound cargo under their respective domestic security protocols (DHS, 2011). In June 2012, TSA and the European Commission announced an unprecedented air cargo security partnership resulting in U.S. recognition of screening programs in the European Union (E.U.) and Switzerland, paving the way for improved information sharing, stronger security, and more efficient transportation of cargo between the U.S. and Europe. This partnership is particularly significant given that air cargo traffic between the E.U. and the U.S. amounts to over a million tons a year travelling each way across the Atlantic (TSA, 2012).

Alternatively, standardization can be fostered through a process known as "co-creation." Through this approach, government agencies and—in some cases—private industry, work together to develop security policy. By seeking industry input, government is able to identify operational impacts, such as increased costs and supply chain delays that could reduce business efficiency and

hinder economic growth (Mullen, Case Study: The Air Cargo Advance Screening Project, 2013). Co-creation is a hallmark of the success enjoyed by the ACAS Pilot, as collaboration between CBP and TSA was complimented by close involvement of key private sector stakeholders (e.g., Airlines for America, Express Association of America).

"Any government-held intelligence of concern regarding a specific shipment must be shared with private sector ACAS participants when appropriate."

— Mike Mullen, Executive Director, EAA

Public to Private Sector Data Sharing

Despite the benefits of co-creation, security concerns do pose a challenge to free flow of information between government agencies and the private sector. Many industry leaders, including Express Association of America (EAA) Executive Director, Mike Mullen, feel that government should work with the private sector to develop a more robust intelligence-sharing capability. In the case of the ACAS Pilot, such improvements will help ensure that commercial responses to a live terrorist incident are operationally effective (i.e., disrupt the attack), while making the private sector aware of long-term trends that may suggest how their resources are being targeted (Mullen, Proc. of Committee on Homeland Security Subcommittee on Transportation Security United States House of Representatives, 2012).

To relay information regarding terrorist threats to industry, intelligence agencies should provide annual or semi-annual briefings to appropriately cleared company representatives. Such briefings could foster the ongoing dialogue needed to ensure that timely connections are made between trends identified by industry-based security groups and their counterparts in government. Regular, bi-lateral channels of communication must exist between corporate security departments and specific points of contact in the government if critical security information on high-risk shipments is to be shared quickly enough to thwart an imminent attack (Mullen, IDGA Cargo Security Summit ACAS Information, 2014).

Inter-Agency Collaboration

Challenges related to seamless information sharing and co-creation do not only affect the public-private sector dynamic. On the contrary, collaboration between government agencies has proven problematic over the years—despite some exceptions, including the ACAS Pilot. In fact, Brad Elrod of Pfizer Global Logistics Compliance stated that the biggest flaws of U.S. supply chain integrity policy do not rest with any single domestic program, but with a general lack of coordination among government agencies to better integrate security and documentation requirements (Elrod, Securing Chemical Inventory: Safety First at Pfizer). Today, government agencies are trying harder than ever to coordinate their efforts, but it is difficult to find a truly universal approach as the focus and needs of each agency vary substantially (Elrod, The Role of the Federal Government in Securing Chemical Inventory, 2013). For example, CBP's historic focus is on securing cargo so it is free of drugs and other prohibited items, whereas TSA is entrusted with identification of IEDs and other threats to the safety of the traveling public. It is rare that two agencies with such divergent end-goals are able to coordinate effectively. Nevertheless, agencies must recognize that though they may be responsible for disparate elements of national security, they share a single mission—securing the American people. Thus, government agencies should harness and coordinate their individual strengths with this realization in mind.

Conclusion

In a final evaluation, the potential for a serious cargo security breach poses a significant threat to the U.S. that could result in substantial personal and financial loss. While more conventional use of cargo as a weapon (e.g., the Lockerbie bombing) is well recognized, the risk of unintended casualties due to mismanagement of stolen consumable goods, such as pharmaceuticals, is no less disturbing. Indeed, it possible that large scale theft and intentional tampering of such products—or their replacement with counterfeits—could serve as a new mode of terrorist attack. Were potential loss of life not enough, the financial ramifications of a cargo security breach are equally staggering. Domestic cargo theft costs American corporations hundreds of millions of dollars annually with international losses extending to the billions. The forfeiture of such revenue is particularly alarming as the U.S. pursues a fragile recovery following the Great Recession.

Given the enormity of these risks and increasing adversary sophistication, private and public sector stakeholders have worked diligently to mitigate this threat. In fact, technological advances, including enhanced GPS and geo-fencing capabilities, permit unprecedented monitoring of cargo as it moves across the globe. Meanwhile, improved data availability, sharing, and analysis allows targeting of high-risk shipments early in the supply chain, preventing bottlenecks and fostering efficient use of limited resources. A prime example of such data collaboration is the ACAS Pilot, which leverages the expertise of two major Federal agencies (i.e., CBP and TSA).

While these advances have enhanced supply chain security, the need for substantial change remains. The U.S. must continue to promote international harmonization of cargo security programs, thereby maximizing security while streamlining the regulatory burden placed on the private sector. Such harmonization can only be obtained through strong partnerships with foreign commercial and government stakeholders. Put simply, limited U.S. jurisdiction and the complexity of international trade make collaboration essential. A final outstanding challenge is fluid communication between government security agencies and their private sector counterparts. While appropriate levels of operational security must be followed, the need for effective, real-time knowledge sharing cannot be ignored. Similarly, government agencies should build on past success by identifying collaboration opportunities that advance national security.

In light of recent cargo security improvements, it is likely these outstanding issues will be addressed by key players in the global supply chain. However, thought leaders must continue to promote this cause if the sweeping changes needed to further mitigate this vulnerability are to be realized. Indeed, it is only through ongoing debate, analysis, and collaboration that policy makers and industry leaders can hope to secure the American people while fostering an environment that remains conducive to the free movement of goods.


45

Works cited

Applebome, P.
(2012, May 3). 2 Brothers Accused in Huge Theft of Prescription Drugs. Retrieved January 10, 2014, from The New York Times: http://www.nytimes.com/2012/05/04/nyregion/2-brothers-arrested-in-10-theft-of-80-million-in-prescription-drugs.html?_r=0

Associated Press.
(2013, September 2013). Chicago Tylenol murders remain unsolved after more than 30 years. Retrieved February 2014, 2014, from Fox News Online: http://www.foxnews.com/us/2013/09/28/chicago-tylenol-murders-remain-unsolved-after-more-than-30-years/

Bartz, S.
(2012). The Tylenol Mafia: Marketing, Murder, and Johnson & Johnson. CreateSpace.

Chambers, D.
(2013). Opportunities and Challenges in Global Trade. IDGA Cargo Security Summit. Baltimore.

Cobb, M.
(2013). In-Transit Security & Technology. IDGA Cargo Security Summit. Baltimore.

DHS.
(2011). DHS Progress in 2011: Strengthening International Partnerships. Retrieved January 29, 2014, from Department of Homeland Security: https://www.dhs.gov/dhs-progress-2011-strengthening-international-partnerships

DHS.
(2014). Securing the Homeland, Strengthening the Nation. Retrieved January 15, 2014, from The FY14 Budget in Brief: www.dhs.gov

Efrati, A., & Loftus, P.
(2010, March 17). Lilly Drugs Stolen in Warehouse Heist. Retrieved January 29, 2014, from The Wall Street Journal: http://online.wsj.com/news/articles/SB10001424052748704688604575125522684707974

Elrod, B.
(2013). The Role of the Federal Government in Securing Chemical Inventory. IDGA Cargo Security Summit. Baltimore.

Elrod, B.
(n.d.). Securing Chemical Inventory: Safety First at Pfizer. Retrieved February 20, 2014, from Http://www.future-artillery.com/Media/7520/11644.pdf

Forsaith, C.
(2013). Mitigating Market Risks and Cargo Theft. IDGA Cargo Security Summit. Baltimore.

Forsaith, C.
(2014, February 6). Pharmaceutical Supply Chain Security. (J. Lewitz, Interviewer)

Gina, A., & Farrely, A.
(2013). Border Management in the 21st Century. IDGA Cargo Security Summit. Baltimore.

Jones, D.
(2013). Hi-Jacking Havens: The Challenges of Moving Cargo in Brazil and Mexico. IDGA Cargo Security Summit. Baltimore.

Kennally, C.
(2012, March). Air Cargo Advance Screening Pilot Strategic Plan. Retrieved January 29, 2014, from Department of Homeland Security: http://www.cbp.gov/sites/default/files/documents/acas_psplan_3.pdf

Mullen, M.
(2012, April 18). Proc. of Committee on Homeland Security Subcommittee on Transportation Security United States House of Representatives. Retrieved January 29, 2014, from Homeland Security Subcommittee: http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Mullen.pdf

Mullen, M.
(2013). Case Study: The Air Cargo Advance Screening Project. IDGA Cargo Security Summit. Baltimore.

Mullen, M.
(2014, January 31). IDGA Cargo Security Summit ACAS Information. (M. Welch, Interviewer)

Parker, N.
(2013). Opportunities and Challenges in Global Trade. IDGA Cargo Security Summit. Baltimore.

Radford, A.
(2014). Creating Actionable Answers. IDGA Cargo Security Summit. Baltimore.

Schuster, E.
(n.d.). Track and Trace in the Pharmaceutical Supply Chain. Retrieved January 29, 2014, from MIT: http://web.mit.edu/edmund_w/www/APICS%20Pharma%20Counterfeit%20EWS%206-30-03).pdf

TSA.
(2012, June 1). TSA and EU Achieve Unprecendented Air Cargo Security through Agreement. Retrieved January 29, 2014, from Transportation Security Administration: http://www.tsa.gov/press/releases/2012/06/01/tsa-and-eu-achieve-unprecedented-air-cargo-security-through-agreement

Contacts

For additional information regarding the content of this report, please contact:

Bob Jacksta
Deloitte Consulting LLP
+1 571 227 8022
rjacksta@deloitte.com

David Solomon
Deloitte Consulting LLP
+1 571 227 8265
dasolomon@deloitte.com

Contributing Authors:

- **Jake Lewitz,** Deloitte Consulting LLP
- **Mansi Shah,** Deloitte Consulting LLP
- **Maura Welch,** Deloitte Consulting LLP

For more information on IDGA, contact:

Tyler Baylis
+1 646 502 3267
tyler.baylis@idga.com