Risk-Based, Layered Approach to Supply Chain Security

Fiscal Year 2010 Report to Congress

April 13, 2010

Homeland Security

U.S. Customs and Border Protection

Message from the Deputy Commissioner of CBP

April 13, 2010

U.S. Customs and Border Protection (CBP) respectfully submits the following report, "Risk-Based, Layered Approach to Supply Chain Security."

The report has been compiled pursuant to language set forth in House Report 111-157 and Conference Report 111-298 accompanying the Fiscal Year 2010 Department of Homeland Security Appropriations Act (P.L. 111-83).

This report explains how CBP achieves meaningful cargo and supply chain security in the absence of the total scanning requirement by employing a risk-based, layered approach.

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable David E. Price
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Harold Rogers
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Robert Byrd
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable George V. Voinovich
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Inquiries relating to this report may be directed to me at 202-344-2001 or to the Department's Deputy Chief Financial Officer, Peggy Sherry, at 202-447-5751.

Sincerely,

David V. Aguilar
Deputy Commissioner
U.S. Customs and Border Protection

Executive Summary

This report responds to the language in the House Report 111-157 and the Conference Report 111-298 accompanying the Fiscal Year (FY) 2010 Department of Homeland Security Appropriations Act (P.L. 111-83) that U.S. Customs and Border Protection (CBP) provide a report by February 1, 2010, on its strategy to achieve meaningful and effective cargo and supply chain security in lieu of 100-percent scanning of cargo. CBP agrees with Congress's conclusion that, "at least for now, a 100-percent scanning goal is not feasible, and even if it were, would come at an unacceptably high cost monetarily and in the displacement of other efforts."

The motivation behind the 100-percent scanning provision, and one of our principle national security interests, is to prevent adversaries from smuggling a nuclear weapon into the United States for the purposes of an attack. CBP has determined that a risk-based and layered approach to enhancing security across all potential transit vectors (air, land and sea) is more efficient and cost effective than alternative approaches that focus exclusively on a single layer of defense. Even if scanning could guarantee the security of every maritime container, focusing all efforts and resources on a single layer (containerized cargo) within a single vector (maritime) does not address the vulnerabilities associated with other potential vectors.

As opposed to a 100-percent scanning approach, which relies almost exclusively on technology to enhance the security of maritime containerized cargo, CBP must work to detect, prevent or deter attacks against or the exploitation of the supply chain by utilizing technologies where appropriate, but also by relying on layers of non-sensor based programs across air, land and maritime pathways. Some of these additional layers include:

- Advanced information under the 24-Hour Rule and Trade Act of 2002 (P.L. 107-210; supplemented now by CBP's proposed Importer Security Filing (ISF), or "10+2" requirements)
- Screening the information through the Automated Targeting System (ATS) and National Targeting Center - Cargo (NTC-C)
- Partnerships with industry and the private sector such as the Customs Trade Partnership Against Terrorism (C-TPAT)
- Partnerships with foreign governments, such as the Container Security Initiative (CSI) and the Secure Freight Initiative (SFI)
- Use of Non-Intrusive Inspection (NII) technology and mandatory exams for all high-risk shipments

The goal of this layered approach is to combine all of these systems to allow CBP to receive, process and act upon commercial and security information in a timely manner so that we can accurately target, in a highly systemized fashion, suspect shipments without hindering the movement of commerce through U.S. ports. Different layers focus on securing different parts of the supply chain, ensuring that cargo is regularly assessed and that security does not rely on any single point that could be compromised.

CBP continuously works to refine this layered process. Given the constantly evolving nature of the key components of the global supply chain, its complexity, size and its potential value as a target of terrorist attack or exploitation, frequent reviews and assessments of its security and efficiency are necessary. Ongoing efforts focus on strengthening existing tools, identifying needs for additional security measures and ensuring the implementation of priority goals in light of both the wide range of threats we face and the balance CBP must maintain between critical security and expediting missions.

While the 100-percent maritime cargo scanning mandate is unlikely to be achieved by the 2012 deadline, if ever, CBP has taken and will continue to take concrete steps to ensure the security of goods transiting our Nation's borders. This report outlines this progress. In addition, ongoing assessments are underway to determine the best utilization of technologies to scan maritime containers abroad and, perhaps more important, to determine the best mix of scanning and other non-sensor programs (such as partnerships with industry and foreign governments, international standards and advance information) to enhance security across air, land and sea vectors.

Risk-Based Layered Approach to Supply Chain Security

Table of Contents

I. Legislative Language

This document responds to the reporting language set forth in the House Report 111-157 and the Conference Report 111-298 accompanying the Fiscal Year (FY) 2010 Department of Homeland Security (DHS) Appropriations Act (P.L. 111-83).

Conference Report 111-298 states:

> The conference agreement provides $162,000,000 for International Cargo Screening as proposed by the House, instead of $165,421,000 as proposed by the Senate. The conferees strongly support current efforts to reduce the vulnerability of international supply chains being used to smuggle illicit weapons, or being disrupted by such weapons. However, the conferees also recognize practical difficulties in trying to meet the statutorily mandated target of 100 percent scanning of U.S.-bound cargo in foreign ports. The conferees therefore direct CBP to report, not later than February 1, 2010, on its strategy to achieve meaningful and effective cargo and supply chain security, as described in the House report.

House Report 111-157 states:

> While cargo security efforts should not be tied to one model, the threat of trade supply chains being used to move weapons, or to be themselves a target for economic disruption, remains. A number of programs help contribute to security in this regard, including the Customs-Trade Partnership Against Terrorism (C- TPAT), the new security filing (10+2) rule, and improved exchange of information with friendly governments. However, assuming that 100 percent overseas scanning is not likely soon, if ever, to be achieved, it is not clear what mix of measures the Department assumes it should work toward to take its place. Might SFI be the best approach, based on the risk, for ports in high threat areas? How permanent a solution is CSI, and what is its optimal end-state? The Committee directs CBP to report, not later than January 15, 2010, on its strategy to achieve meaningful cargo and supply chain security in the absence of the total scanning requirement.

II. Background

Since 2006, there have been two major pieces of legislation addressing 100-percent scanning of U.S.-bound containers.

- Section 231 of the Security and Accountability For Every Port Act of 2006 (P.L. 109-347; SAFE Port Act) required the Department to establish a pilot program in three foreign ports that coupled NII and Radiation Portal Monitors (RPMs) to scan for radioactive and nuclear material all U.S.-bound containers laden in those ports.

- Section 1701 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53; 9/11 Act) amended section 232 of the SAFE Port Act to mandate that by July 12, 2012, a container loaded on a vessel in a foreign port shall not enter the United States unless that container was scanned by NII and radiation detection equipment before it was loaded onto the vessel.

"Scanning" is defined in the SAFE Port Act as subjecting the maritime container to non-intrusive imaging, radiation detection, or both. In practice, the radiation scan is conducted using an RPM, while the non-intrusive imaging is achieved through a large-scale X-ray or gamma-ray device that shows the contents of the container and the presence of any anomalies that could present concern.

Section 232 of the SAFE Port Act, as amended by section 1701(a) of the 9/11 Act provides the Secretary with flexibility to extend the 2012 deadline in two-year increments, with no limit on the number of extensions that may be granted, provided at least two of the following six pre-defined conditions exist:

> (1) Systems to scan containers are not available for purchase and installation.
> (2) Systems to scan containers do not have a sufficiently low false alarm rate for use in the supply chain.
> (3) Systems to scan containers cannot be purchased, deployed or operated at ports overseas including, if applicable, because a port does not have the physical characteristics to install such a system.
> (4) Systems to scan containers cannot be integrated, as necessary, with existing systems.
> (5) Use of systems that are available to scan containers will significantly impact trade capacity and the flow of cargo.
> (6) Systems to scan containers do not adequately provide an automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel.

Extensions will be necessary as the 2012 deadline draws near. In several reports to Congress beginning in 2007, DHS and CBP delineated the multitude of challenges associated with 100-percent scanning. Several technical, logistical and diplomatic challenges prevent DHS from fully realizing the congressional mandate of the 9/11 Act:

- Technical: Sustaining equipment operations in extreme weather conditions; addressing health and safety concerns; and protecting data privacy.
- Logistical: Re-configuring port layouts to accommodate the equipment without affecting port efficiency; determining who will bear the costs for buying, operating and maintaining the scanning equipment; and developing local response protocols for adjudicating alarms.
- Diplomatic: Concluding agreements and arrangements with partnering governments and terminal operators who will own and operate the scanning equipment; and addressing the potential requirement for reciprocal scanning of U.S. exports.

Furthermore, budgetary challenges exist as the costs of 100-percent scanning are prohibitive. Deploying SFI-type scanning equipment would cost about $8 million per lane for the more than 2,100 shipping lanes at more than 700 ports around the world that ship to the United States. On top of these initial costs, operating costs would be very high. These include only DHS expenses, not the huge costs that would be borne by foreign governments and industry.

Considering these issues, CBP concurs with the House Report language, which states, "at least for now, a 100-percent scanning goal is not feasible, and even if it were, would come at an unacceptably high cost monetarily and in the displacement of other efforts." As such, this report complies with the direction of the House Report to explain how CBP achieves meaningful cargo and supply chain security in the absence of the total scanning requirement.

III. Discussion

Discussion of meaningful supply chain security necessarily describes CBP's efforts employed in a layered approach to ensure the integrity of the supply chain from the point of stuffing through CBP clearance or re-exportation at a U.S. port of entry. This multi-layered approach includes:

- Advanced information under the 24-Hour Rule and Trade Act of 2002 (supplemented now by our ISF, or "10+2" requirements) and screening the information through the ATS and NTC-C;
- Partnerships with industry and the private sector such as C-TPAT;
- Partnerships with foreign governments, such as the CSI and SFI; and
- Use of NII technology and mandatory exams for all high-risk shipments.

The goal of this layered approach is to combine each of these systems to allow us to receive, process and act upon commercial information in a timely manner so that we can target, in a very specific fashion, the suspect shipments without hindering the movement of commerce through our ports.

A. Advanced Information

Absolutely critical to securing the supply chain is receiving information on shipments prior to the lading of the cargo on U.S.-bound vessels, screening this information through the ATS and CBP acting on the information in a strategic manner. This strategy allows for the facilitation of legitimate trade, while focusing resources on shipments of concern.

1. ATS

CBP focuses on two general strategies to identify and interdict high-risk shipments. The first strategy, commonly referred to as targeting "knowns," is to identify shipments that are related to parties or individuals that are known or suspected to be involved in illicit activities. Cargo shipment information processed through the ATS is compared to various databases including watch lists, sanctions lists and law enforcement records to identify such possibly related shipments. The second strategy, commonly referred to as targeting "unknowns," is to identify shipments for which there is no specific derogatory information but which display patterns indicative of high-risk behaviors.

Advance electronic cargo information is used to gather, fuse and assess data from the global supply chain; develop a risk profile; and evaluate that risk at the earliest point. The advance electronic data requirements (commonly referred to as the 24-Hour Rule) were part of the Trade Act of 2002, and established uniform minimum requirements for transmitting cargo data to CBP. CBP also incorporates the entry information provided by the importers into ATS. As will be discussed further, ATS also incorporates the additional ISF data elements provided by the ISF importers and ocean carriers.

CBP uses ATS to collect and analyze cargo shipping data, as well as to identify and select high-

risk shipments for further review and examination. ATS targeting concepts are based on major risk factors, such as familiarity indicators, geographic routing and addresses, violation history, high-risk commodities and intelligence.

- **Familiarity interdictors** take into account frequency and volume of trade activity, entity identification and certification as a trusted entity by means of confirmed participation in the C-TPAT program.
- **Geographic routing concepts** take into account the points of origin, places of receipt, ports of lading and conveyance routes based on countries of interest. ATS also utilizes a country tier model that ranks each country on the basis of potential terrorism-related threats.
- **Violation history** is based on matches of names and addresses to law enforcement databases. These matches are tiered on the basis of the severity of the records.
- **High-risk commodities** are defined as those that, on the basis of the context of the importation, pose an immediate or potential threat to the homeland. These high-risk commodities include conventional weapons, ammonium nitrate, chemicals and chemical precursors, biological materials and nuclear, radiological and dual-use items. Shipments to legitimate importers of these commodities are generally not considered high-risk and may not necessarily be designated for examination. However, such shipments to unknown parties or in the presence of other high-risk factors may lead to further scrutiny.
- **Intelligence** drivers are based on strategic risk assessments, analysis of smuggling patterns and concealment methods and the most current threat information.

Using these factors, CBP targeting is and must be flexible. It can be adapted to meet changing conditions or to respond to emerging threats.

2. ISF

As the rule sets and targeting through ATS continually evolve and adapt to threats, CBP has also undertaken an effort to bolster the information received on shipments for anti-terrorism targeting purposes. Through the ISF or "10+2", CBP significantly increases the scope and accuracy of information gathered on the goods, conveyances and entities involved in the shipment of cargo arriving by vessel into the United States. Generally, the ISF requires importers to supply CBP with 10 trade data elements 24 hours prior to lading for cargo shipments that will be arriving into the United States by vessel. The ocean carriers are required to provide their vessel stow plans and container status messages to CBP electronically. This effort was codified in Section 203 of the SAFE Port Act, which mandated the development of a regulation to require additional data elements for improved high-risk targeting, including appropriate security elements of entry data to be provided as advanced information prior to vessel lading.

After several years of internal development and proactive consultation with industry stakeholders, CBP's ISF rule was published as an interim final rule (IFR) on November 25, 2008, at 73 Federal Register 71,730 and became effective on January 26, 2009. In the IFR, six of the 10 data elements were made flexible so that the trade could acclimate to the requirements. Those flexibilities reflected a need to submit either a range of possible responses or to submit within a flexible timeframe. The data elements with flexibilities include:

- Ship To Party
- Manufacturer (Supplier) name/address
- Country of Origin
- Commodity Harmonized Tariff Code – six digit level
- Container Stuffing Location
- Consolidator name/address

The other requirements of the ISF were made final in the IFR and include:

- Importer Security Filing Elements
  - Importer of Record Number
  - Consignee Number
  - Buyer (Owner) name/address
  - Seller (Owner) name/address
- Additional Carrier Requirements (2 data sets):
  - Vessel Stow Plans
  - Container Status Messages

The ISF data supplied to CBP is added to the shipment record information in ATS and is available to support the targeting efforts of CBP personnel.

CBP is currently conducting a structured review and is analyzing the six "flexible filing" data elements. In the near future, CBP, in coordination with other parts of the Executive Branch, will determine whether to eliminate, modify or leave unchanged the "flexible filing" options as it works towards finalizing the "10+2" Rule.

The full compliance (enforcement) date for the "10+2" requirements commenced on January 26, 2010, thus ending a 12-month delayed enforcement period. CBP implemented the 12-month delayed enforcement period to provide the trade community with time to adjust their business processes in order to comply with "10+2" rule, as well as provide extensive educational outreach on the new requirements. During the first few months of full enforcement, CBP does not anticipate assessing liquidated damages, monetary penalties or issuing "do not load" (DNL) messages for compliance reasons. However CBP reserves the right to take any necessary enforcement actions, including DNLs, whenever there is a national security reason for doing so.

This approach to fully informed compliance reflects CBP's desire to work with the trade to ensure that all parties are able to submit the required information. It will be a critical addition to CBP's targeting and a necessary enhancement to the layered approach to secure the supply chain.

3. NTC-C

To bring together much of this advanced information, CBP built the NTC-C, a critical tool in CBP's layered enforcement strategy. NTC-C leverages open source, classified and unclassified information of a law enforcement and commercial nature to proactively target and coordinate examinations of high-risk cargo on all modes of transport 24 hours per day, seven days per week.

To facilitate national security targeting, the NTC-C has several teams that perform advanced work and functions. Personnel at the NTC-C conduct in-depth research, compile the information and target various entities identified using:

- ATS
- Automated Commercial System
- TECS records
- TECS Memorandum of Information Received reports

Among other initiatives, teams at the NTC-C also:

- Exploit information received from National Targeting Center – Passenger on Terrorist Screening Database and Violent Gang and Terrorist Organization File matches encountered at CBP ports to identity cargo shipments and businesses linked to these individuals.
- Target businesses and individuals involved in the shipment of goods that may have connections to terrorism or involve revenue financing of other illegal activities aiding terrorist organizations.
- Isolate high-risk shipments in the export environment by targeting exports of proliferation concern, including items controlled under the Office of Foreign Assets Control, International Trafficking in Arms Regulations and Commerce Control List originating or transshipping the United States.
- Collaborate with the Defense Intelligence Agency, U.S. Department of Agriculture and other government agencies utilizing the Agricultural Resource Atlas data to target entities with derogatory information that indicates that they have the capability and knowledge to utilize biological materials for illicit purposes.
- Identify drug trends, conduct tactical post seizure analysis, targets involved persons and disseminate intelligence products to CBP, DHS and other government agencies. In addition to targeting for heroin, cocaine and marijuana, the NTC-C Narcotics Unit also has nationwide responsibility for targeting precursor chemicals used for the production of methamphetamines, ecstasy and other dangerous drugs.
- Provide technical advice, facilitate and coordinate the deployment of technical assets and provide assistance to field personnel requiring technical assistance adjudicating issues that potentially involve chemical, biological, radiological, nuclear and explosive Weapons of Mass Destruction threat materials. These functions are conducted by the CBP Laboratories and Scientific Services Teleforensic Center.

In addition to these efforts, the NTC-C fosters partnerships that help to provide a robust targeting environment. Examples include:

- Operation Wing Clip (OWC): OWC is a multi-agency initiative created in 2006 and led by the U.S. Immigration and Customs Enforcement's (ICE's) Forensic Document Laboratory. OWC develops intelligence and operational leads based on documents intercepted and seized by CBP Officers at international mail and express consignment courier facilities. Officers intercept documents from countries of interest relating to terrorism, organized crime and human smuggling. NTC-C conducts research on seized

- NTC-C personnel also work closely with ICE and U.S. Drug Enforcement Administration (DEA) to disrupt transnational narcotic organizations by conducting research, targeting shipments and coordinating enforcement activities. NTC-C, ICE and DEA are engaged in collaborative efforts to combat illegal drug trafficking by enhancing data sharing and liaison exchanges
- Through the NTC-C, CBP has been increasing communication and collaboration with the Customs Heads of Intelligence member countries of Australia, Canada, New Zealand and United Kingdom by passing real time tactical information and participating in cargo targeting operations.
- International Cargo Targeting Fellowship: The NTC-C assists CBP's international partners in developing systems to manage anti-terrorism and security threats by hosting foreign Customs officials under the International Fellowship Program. This partnership allows for the sharing of information and best practices, which can maximize the security and facilitation of the international trade supply chain. The objective is the refinement of targeting techniques to identify high-risk shipments.

B. Partnerships

While the NTC-C partnerships help to improve the collection and use of advanced information, CBP also has initiated several partnerships with industry and foreign governments to help improve security of the supply chain.

1. C-TPAT

The C-TPAT program is another critical layer in CBP's multi-layered cargo enforcement strategy. Through this program, CBP works with the trade community to adopt tighter security measures throughout their international supply chains. In exchange for adopting stronger security practices, and after verification by CBP Supply Chain Security Specialists (SCSSs) that the measures are in place, CBP affords these members reduced risk of inspection.

The C-TPAT program uses a "trust but verify" approach with the trade community. A prospective member company submits basic company information and a security profile via an Internet-based portal system. CBP conducts records checks on the company in its law enforcement and trade databases, then evaluates the security profile, in order to ensure that the company meets the minimum security criteria for its particular business sector. Those member companies that pass initial vetting are certified into the program. Using a risk-based approach, SCSSs conduct on site visits of foreign and domestic facilities to confirm that C-TPAT security practices are in place and operational.

Congress codified C-TPAT and established certain time sensitive mandates such as reviewing and certifying security profiles within 90 days of submission, conducting validations within one year of certification and conducting revalidations within four years of the initial validation. C-TPAT managers are responsible for ensuring compliance with these time frames as well as the timeliness, thoroughness and accuracy of validation reports.

Currently, membership in C-TPAT consists of 9,509 certified partners, which includes 4,330 importers, 2,583 carriers, 821 brokers, 784 consolidators/third party logistic providers, 56 marine port authority and terminal operators and 935 foreign manufactures. Furthermore, C-TPAT has conducted 13,246 on-site validations of manufacturing and logistics facilities in 89 countries representing some of the most terrorist prone and high-risk areas of the world. Additionally, 301 C-TPAT importer partners have been designated as Tier 3, meaning they have exceeded the minimum security criteria have been granted the highest level of program benefits.

In accordance with World Customs Organization Framework of Standards, C-TPAT has been working with several foreign customs administrations to align with their industry partnership programs, which effectively allows CBP to internationalize the core principles of the C-TPAT program and create global cargo security standards. As a result, CBP has signed Mutual Recognition Arrangements with New Zealand, Canada, Jordan and Japan. CBP has also provided technical assistance to several other customs administrations.

2. CSI

Through CSI, CBP is able to combine advanced information and targeting capabilities through partnerships with Customs regimes across the globe. CSI works to ensure that all containers posing a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels destined for the United States. CSI teams in foreign ports consist of CBP Officers, ICE Special Agents and Intelligent Research Specialists.

CSI is currently operational at 58 ports covering more than 80 percent of the maritime containerized cargo bound for the United States. CSI teams located in the foreign ports are supplemented by personnel at the NTC-C and work to review 100 percent of the bills of lading in order to identify those containers that pose a high risk for terrorism. CBP then coordinates with host government personnel to mitigate that risk by garnering additional information on the shipment or requesting further examination.

C. SFI

In addition to CSI personnel, CBP has established further presence overseas with SFI and attempts to scan 100 percent of U.S.-bound, maritime containers in foreign ports. However, as noted in this and previous congressional reports, there are significant challenges associated with 100-percent scanning, and CBP has submitted several reports explaining those challenges. However, a strategic deployment of scanning systems to certain locations can help to augment the layered approach to supply chain security. As such, SFI, through partnerships with foreign governments, terminal operators and carriers, enhances CBP's capability to better assess the security of U.S.-bound, maritime containers by scanning them for special nuclear and other radioactive materials before they are laden on vessels bound for the United States. An integrated scanning system, consisting of an RPM provided by the U.S. Department of Energy's National Nuclear Security Administration and a NII imaging scanner provided by CBP, collects and aggregates container data. These data are then linked to the associated container using optical character recognition technology and analyzed by CBP officers who determine if the container should be referred to the host nation for secondary examination prior to lading.

Currently, SFI has scanning systems deployed in Qasim, Pakistan; Southampton, United Kingdom; Puerto Cortes, Honduras; and Busan, Korea. Soon, SFI will become operational in Salalah, Oman. Initial locations have provided valuable lessons learned and form the basis of prior reports to Congress. The data from these operations will help to inform future deployments to strategic locations. Further, as with any operation, CBP must continually evaluate the usefulness of these deployments and consider whether the continuation of scanning operations adds value in each of these locations. Integral to this evaluation would be the identification of potential additional locations that would strategically enhance CBP efforts.

D. Domestic Technology Deployments

In conjunction with CBP's many other initiatives discussed in this report (C-TPAT, ATS, NTC, 24-Hour Rule, CSI, etc.), domestic deployments of technology allow CBP personnel to work smarter and faster in recognizing potential terrorist threats.

Technologies currently deployed to our Nation's land, sea and air ports of entry include large-scale X-ray and gamma-ray imaging systems, as well as a variety of portable and handheld technologies, including radiation detection technology. NII technologies are viewed as force multipliers that enable us to scan or examine a larger portion of commercial traffic for the presence of contraband, while facilitating the flow of legitimate trade, cargo and passengers. NII systems, in many cases, give CBP the capability to perform thorough examinations of cargo without having to resort to the costly, time-consuming process of unloading cargo for manual searches or intrusive examination of conveyances by methods such as drilling or dismantling.

On September 11, 2001, a total of 64 large-scale NII systems were deployed to our Nation's ports of entry, and none was deployed to the Northern border. Today, a total of 232 NII systems are deployed, including 48 systems on our common border with Canada. This rapid deployment of NII technology was accomplished by simplifying the acquisition process to reduce costs, improve effectiveness and make maximum use of available commercial off-the-shelf technology.

Currently, the 232 large-scale NII systems deployed to our ports of entry include 30 Vehicle and Cargo Inspection Systems (VACIS), 71 Mobile VACIS, 24 Rail VACIS, eight Truck X-ray, 16 Mobile Truck X-ray, 19 Pallet Gamma-ray, eight Portal VACIS, one High-Energy Fixed X-ray System, 36 High-Energy Mobile X-ray Systems, 16 Z-Backscatter Vans, two Mobile GaRDS units, and one Z-Portal System. Of the 232 large-scale NII systems deployed, 48 are deployed on the northern border including one at an airport, 94 are deployed on the southern border, one is deployed at the Federal Law Enforcement Training Center and 90 are deployed to seaports.

CBP has used the deployed systems to conduct over 37 million examinations, resulting in over 8,300 narcotic seizures with a total weight of over 2.5 million pounds of narcotics. Furthermore, over $27 million in undeclared currency has been seized utilizing deployed NII systems.

In addition to the 232 NII systems currently in its inventory, CBP will continue to deploy additional systems to United States ports of entry. CBP considers factors such as available intelligence, traffic volumes, types and density levels of imported commodities, port

infrastructure constraints, appropriate mixes of equipment and currently available off-the-shelf technology and cost effectiveness, to determine how best to utilize its resources.

Further complimenting the layered approach is the deployment of RPMs to our ports of entry to scan for illicit radiological/nuclear materials. Currently, CBP has 434 RPMs deployed at priority seaports in the United States, through which approximately 99 percent of all arriving sea-borne containerized cargo passes. Additionally, CBP currently has 491 RPMs on the northern border, which provides the capability to scan 100 percent of truck cargo. CBP also scans 100 percent of truck cargo on the southern border with 391 RPMs deployed.

Used in combination with our layered enforcement strategy, these tools currently provide CBP with a significant capability to detect contraband, including illicit nuclear or radiological materials.

IV. Conclusion

As noted in this report, CBP employs an effective risk-based, layered approach to securing the global supply chain. Advanced information is screened using automated systems and analyzed by trained personnel in order to provide actionable information to CBP Officers. The screening and analysis of this information allows CBP to focus its resources on those shipments of concern, while facilitating the movement of legitimate cargo. In addition to receiving advanced information, CBP partners with industry members to enhance their own security practices throughout the international supply chain. Foreign government partnerships also provide invaluable insight into potentially harmful shipments and, in some locations, have allowed CBP to deploy scanning systems to scan containers for radiation. Finally, CBP has positioned technology at all ports of entry that serve as force multipliers for officers in the field. Taken in combination, these layers provide meaningful supply chain security.

Dependency on one solution or one layer of risk assessment is not a responsible approach to supply chain security. CBP has consistently maintained that 100-percent scanning does not equal 100-percent security. The utilization of technologies, such as the scanning systems deployed under SFI, represent one of several layers within a multi-layered and risk-based strategy.

In several reports and testimony provided to Congress, DHS and CBP have noted the myriad challenges associated with 100-percent scanning. While the additional data elements provided by these scanning systems has benefit, the technological, logistical and diplomatic issues, in addition to the prohibitive costs all indicate that a "100-percent scanning" approach would be difficult to achieve and of questionable value.

However, CBP has in place and continues to refine a variety of security programs to enhance the security of the goods arriving daily at our borders. These programs are organized around two fundamental and guiding principles; namely, the principle that a 'defense in depth' or layered approach is more effective than a single point of security and the principle that risk management is an efficient and effective means to prioritize missions and allocate resources. Only continual enhancement and improvement of these layers will provide the security needed and ensure that CBP's resources are most effectively utilized.

V. Appendix A – List of Acronyms

Acronym	Definition
9/11 Act	Implementing Recommendations of the 9/11 Commission Act of 2007
ATS	Automated Targeting System
CBP	U.S. Customs and Border Protection
CSI	Container Security Initiative
C-TPAT	Customs Trade Partnership Against Terrorism
DEA	U.S. Drug Enforcement Administration
DHS	U.S. Department of Homeland Security
DNL	Do Not Load
ICE	U.S. Immigration and Customs Enforcement
IFR	Interim Final Rule
ISF	Importer Security Filing
NII	Non-Intrusive Inspection
NTC-C	National Targeting Center - Cargo
OWC	Operation Wing Clip
RPM	Radiation Portal Monitor
SAFE Port Act	Security and Accountability for Every Port Act of 2006
SCSS	Supply Chain Security Specialist
SFI	Secure Freight Initiative
VACIS	Vehicle and Cargo Inspection Systems