



U.S. Customs and Border Protection

**Report to Congress on Integrated Scanning System
Pilots (Security and Accountability for Every Port
Act of 2006, Section 231)**

Table of Contents

3 Legislative Requirement/Citation

7 Executive Summary

24 Background

28 Lessons Learned

29 Southampton, U.K.

31 Qasim, Pakistan

31 Puerto Cortes, Honduras

33 Hong Kong

33 Busan, S. Korea

33 Singapore

34 Salalah, Oman

35 Expansion

38 Conclusion

40 Acronyms

Appendix A – Foreign Government SFI Review

Appendix B – Terminal Operator Review of SFI

**Appendix C – International Economics, Inc. (IEC) Review of SFI Impact on Trade
(International Economics, INC.)**

Appendix D – Trade and Industry Review of SFI

Appendix E – Foreign Correspondence Concerning SFI

Legislative Requirement/Citation

In the Security and Accountability for Every Port Act of 2006 (SAFE Port Act), Pub L. No 109-347 (October 4, 2006), Congress directed the Secretary of the Department of Homeland Security (DHS), in coordination with the Secretary of the Department of Energy (DOE), as necessary, and the private sector and host governments when possible, to pilot an integrated scanning system at three foreign ports. Section 231 (d) of the SAFE Port Act requires a report to Congress on the pilot integrated scanning system.

SEC. 231. Pilot Integrated Scanning System.

(a) Designations- Not later than 90 days after the date of the enactment of this Act, the Secretary shall designate 3 foreign seaports through which containers pass or are transshipped to the United States for the establishment of pilot integrated scanning systems that couple non-intrusive imaging equipment and radiation detection equipment. In making the designations under this subsection, the Secretary shall consider 3 distinct ports with unique features and differing levels of trade volume.

(b) Coordination- The Secretary shall—

(1) coordinate with the Secretary of Energy, as necessary, to provide radiation detection equipment through the Department of Energy's Second Line of Defense and Megaports programs; or

(2) work with the private sector or, when possible, host governments to obtain radiation detection equipment that meets both the Department's and the Department of Energy's technical specifications for such equipment.

(c) Pilot System Implementation- Not later than 1 year after the date of the enactment of this Act, the Secretary shall achieve a full-scale implementation of the pilot integrated scanning system at the ports designated under subsection (a), which--

(1) shall scan all containers destined for the United States that are loaded in such ports;

(2) shall electronically transmit the images and information to appropriate United States Government personnel in the country in which the port is located or in the United States for evaluation and analysis;

(3) shall resolve every radiation alarm according to established Department procedures;

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

- (4) shall utilize the information collected to enhance the Automated Targeting System or other relevant programs;
 - (5) shall store the information for later retrieval and analysis; and
 - (6) may provide an automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel.
- (d) Report- Not later than 180 days after achieving full-scale implementation under subsection (c), the Secretary, in consultation with the Secretary of State and, as appropriate, the Secretary of Energy, shall submit a report to the appropriate congressional committees, that includes--
- (1) an evaluation of the lessons derived from the pilot system implemented under this subsection;
 - (2) an analysis of the efficacy of the Automated Targeting System or other relevant programs in utilizing the images captured to examine high-risk containers;
 - (3) an evaluation of the effectiveness of the integrated scanning system in detecting shielded and unshielded nuclear and radiological material;
 - (4) an evaluation of software and other technologies that are capable of automatically identifying potential anomalies in scanned containers; and
 - (5) an analysis of the need and feasibility of expanding the integrated scanning system to other container security initiative ports, including--
 - (A) an analysis of the infrastructure requirements;
 - (B) a projection of the effect on current average processing speed of containerized cargo;
 - (C) an evaluation of the scalability of the system to meet both current and future forecasted trade flows;
 - (D) the ability of the system to automatically maintain and catalog appropriate data for reference and analysis in the event of a transportation disruption;
 - (E) an analysis of requirements, including costs, to install and maintain an integrated scanning system;
 - (F) the ability of administering personnel to efficiently manage and utilize the data produced by a non-intrusive scanning system;
 - (G) the ability to safeguard commercial data generated by, or submitted to, a non-intrusive scanning system; and
 - (H) an assessment of the reliability of currently available technology to implement an integrated scanning system.

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

On August 3, 2007, the President signed the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), Pub. L. No. 110-53. Under Title XVII, titled Maritime Cargo, section 1701 of the 9/11 Act amends section 232 of the SAFE Port Act to require 100 percent scanning of high-risk containers at all foreign ports shipping containers to the United States.

Section 232(a) of the SAFE Port Act, as amended by the 9/11 Commission Act, now reads:

(1) **SCREENING OF CARGO CONTAINERS** — The Secretary shall ensure that 100 percent of the cargo containers originating outside the United States and unloaded at a United States seaport undergo a screening to identify high-risk containers.

(2) **SCANNING OF HIGH-RISK CONTAINERS** —The Secretary shall ensure that 100 percent of the containers that have been identified as high-risk under paragraph (1), or through other means, are scanned or searched before such containers leave a United States seaport facility.

Section 232(b): **FULL-SCALE IMPLEMENTATION** — The Secretary, in coordination with the Secretary of Energy and foreign partners, as appropriate, shall ensure integrated scanning systems are fully deployed to scan, using non-intrusive imaging equipment and radiation detection equipment, all containers entering the United States before such containers arrive in the United States as soon as possible, but not before the Secretary determines that the integrated scanning system—

- (1) meets the requirements set forth in section 231(c);
- (2) has a sufficiently low false alarm rate for use in the supply chain;
- (3) is capable of being deployed and operated at ports overseas;
- (4) is capable of integrating, as necessary, with existing systems;
- (5) does not significantly impact trade capacity and flow of cargo at foreign or United States ports; and
- (6) provides an automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel.

Section 232(c): **REPORT** — Not later than 6 months after the submission of a report under section 231(d), and every 6 months thereafter, the Secretary shall submit a report to the appropriate congressional committees describing the status of full-scale deployment under

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

subsection (b) and the cost of deploying the system at each foreign port at which the integrated scanning systems are deployed.

The 9/11 Recommendations Act establishes the following under its section 1701 regarding container scanning and seals:

General Rule – A container that was loaded on a vessel in a foreign port shall not enter the United States (either directly or via a foreign port) unless the container was scanned by non-intrusive imaging equipment and radiation detection equipment at a foreign port before it was loaded on a vessel.

Timeline – This must be implemented by July 1, 2012, unless a port meets two of several conditions for extension.

Extension Conditions –

- (A) Systems to scan containers are not available for purchase and installation.
- (B) Systems to scan containers do not have a sufficiently low false alarm rate for use in the supply chain.
- (C) 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.
- (D) Systems to scan containers cannot be integrated, as necessary, with existing systems.
- (E) Use of systems that are available to scan containers will significantly impact trade capacity and the flow of cargo.
- (F) 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.

The *9/11 Act* provides the Secretary of DHS with the authority to extend the 2012 deadline in two year increments provided two of the six statutory conditions exist. There is no limit to the number of extensions that can be granted.

Executive Summary

On October 13, 2006, President George W. Bush signed into effect the Security and Accountability for Every (SAFE) Port Act of 2006. The purpose of the Act is to improve maritime and cargo security through enhanced layered defenses, including hardening critical infrastructure, increasing port defenses against possible attacks, and working to ensure the security of the maritime transportation system. The SAFE Port Act provides a comprehensive, strategic vision that touches on all aspects of the existing maritime security architecture -- from securing the containers that transit the supply chain, to defending the vessels and ports that connect it, to ensuring the protection and accountability of the people that work within it. Acknowledging the immediate and lasting consequences that any disruption to the global system will have for the United States and the world, the SAFE Port Act emphasizes a balance between securing America's borders and facilitating legitimate trade and travel.

This SAFE Port Act also codified a number of supply chain security programs that DHS established following the September 11, 2001 terrorist attacks and which continue today. These include the use of advance electronic information and automated systems to assess the risk of every container entering our country; human resources and technology to inspect and scan all high risk cargo; and partnerships with the trade and foreign governments to ensure the security of supply chains beyond our nation's borders. Specifically, the SAFE Port Act statutorily established DHS's advanced information requirements and automated analysis, the Customs-Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative (CSI), and the use of NII technology to scan high-risk shipments. The inclusion of these provisions reflects the Act's support for the current layered, risk-based approach to maritime and cargo security.

These programs form the backbone of U.S. Customs and Border Protection's (CBP) risk-management-based, layered enforcement strategy. To most effectively manage multiple threats to our country, we must direct resources to areas of greatest risk. We are constantly working to refine this layered process by strengthening our tools and capabilities, working to maintain an appropriate balance between the wide range of threats we face and allocating our limited resources accordingly. No single layer or tool in our risk-based approach should be overemphasized at the expense of the others. The strength of the strategy is that it ensures continuous security at multiple nodes in the supply chain, distributing resources so that focus on one threat does not overshadow other vulnerable areas that could also be exploited.

The U.S. Department of Homeland Security (DHS) and the U.S. Department of Energy's (DOE) National Nuclear Security Administration (NNSA), along with the U.S. Department of State (DOS) have taken several strategic steps to enhance the layers of security in place to reduce the risk of potential radiological or nuclear threats reaching the United States.

One new layer is the launch of the Secure Freight Initiative (SFI) in December 2006 and the establishment of the SFI International Container Security (ICS) pilot program.

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

Under the SFI/ICS, an integrated scanning system, consisting of radiation portal monitors (RPM) provided by DOE/NNSA and non-intrusive inspection (NII) imaging systems provided by CBP, is used to scan containers as they move through foreign ports. Through optical character recognition (OCR) technology, data from these systems is integrated and provided to CBP officers who determine if the container should be referred to the host nation for secondary examination prior to lading. For the CBP officers, SFI/ICS provides additional data points that are used in conjunction with advanced manifest data, such as 24-Hour Rule information, Customs-Trade Partnership Against Terrorism information, and the Automated Targeting System to assess the risk of each container coming to the United States.

Meeting the legislative requirements of the SAFE Port Act, the first three SFI ports (Puerto Cortes, Honduras; Port Qasim, Pakistan; and Southampton, United Kingdom) became fully operational on October 12, 2007, and are attempting to scan 100 percent of U.S.-bound maritime containers (the total U.S.-bound container volume at these three ports from October 12, 2007 to February 12, 2008 was 51,937 containers). Furthermore, CBP and DOE are working to pilot scanning equipment in additional diverse environments that provide unique challenges, which may include certain terminals in Hong Kong, Salalah (Oman), Port Busan (South Korea), and Singapore.

Section 231 of the SAFE Port Act requires DHS, in coordination with DOE/NNSA, to report to Congress on a number of topics related to SFI. This report responds to the following five topics:

- an evaluation of the lessons derived from the pilot system implemented under this subsection;
- an analysis of the efficacy of the Automated Targeting System (ATS) or other relevant programs in utilizing the images captured to examine high-risk containers;
- an evaluation of the effectiveness of the integrated scanning system in detecting shielded and unshielded nuclear and radiological material;
- an evaluation of software and other technologies that are capable of automatically identifying potential anomalies in scanned containers; and
- an analysis of the need and feasibility of expanding the integrated scanning system to other container security initiative (CSI) ports (with eight subtopics).

Ten months after the SAFE Port Act became law, Congress passed and the President signed the Implementing the Recommendations of the 9/11 Commission Act of 2007 ("9/11 Act"). Any discussion of the successes and challenges of the smaller scale SAFE Port Act pilots must take into account the new, expanded mandate under Section 1701 of the 9/11 Act, requiring by July 1, 2012, that all maritime containers destined for the United States be scanned (using radiation detection and imaging equipment) in a foreign port prior to lading. The 9/11 Act recognizes that a set of technical and logistical

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

challenges must be addressed in order for the scanning requirement to be achieved in all foreign ports and provides DHS with flexibility to extend the 2012 deadline in two year increments, provided the scanning systems meet two of the following six conditions:

- 1) Are not available for purchase and installation;
- 2) Do not have sufficiently low false alarm rates;
- 3) Cannot be purchased, deployed, or operated at ports overseas, including the absence of the physical characteristics at a port necessary for the installation of such a system;
- 4) Cannot be integrated with existing systems;
- 5) Will significantly impact trade capacity and cargo flow; and
- 6) Do not adequately provide an automated notification of questionable or high-risk cargo.

The purpose of this report is to provide feedback on the deployment of integrated scanning equipment to the initial three pilot ports in Honduras, the United Kingdom, and Pakistan during the six month pilot period beginning in October of 2007. Further, this report details the United States Government's efforts under SFI in four additional locations (Hong Kong, Oman, South Korea, and Singapore). While integrated scanning equipment may not yet be deployed, or is not yet fully operational in each of these additional ports, this report will outline some of the lessons we derived throughout the negotiation processes, construction efforts, and initial testing periods.

Significant Findings

With the three initial SFI pilot ports in Honduras, the United Kingdom, and Pakistan, CBP has focused its efforts on exploring methods by which efficient operation (defined by maximizing the security benefit, minimizing disruptions to port operations, and containing costs) could be achieved within the deadline prescribed by law. The SFI/ICS deployments in Honduras, the United Kingdom, and Pakistan indicate that 100 percent scanning of U.S.-bound maritime containers is possible on a limited scale in low volume ports processing primarily gate traffic, but that this process will be difficult to achieve with transshipped containers delivered to the port facility from the waterside. In these first three ports, the United States government benefited from considerable host nation cooperation, low cargo volumes, low transshipment rates, and technology and infrastructure costs covered primarily by the United States Government (although it is important to note that in Pakistan, the Government of Pakistan funded the building of the inspection facility and covered all construction costs). These accommodating and supportive conditions do not exist in all ports shipping to the United States.

As this report will discuss in more detail, the data obtained by the scanning technology does have the potential to enhance targeting by providing two additional data points

(RPM spectra and NII images) to the information and tools already available to CBP officers (including 24-Hour Rule information and the Automated Targeting System). CBP is committed to a realistic and responsible approach that will incorporate these scan data points into our risk-based methodology in places where the additional information would be of the most benefit to our targeters.

The continuation of operations in some of the current SFI pilot locations will afford CBP the opportunity to further test possible solutions to the complex challenges posed by transshipment and high-volume ports. However, while the data can be useful, expenses are significant, even in these limited environments. While we continue to learn important lessons in these initial pilot locations, CBP will focus future scanning deployments on high-risk trade corridors, which represent the greatest threats to the United States. Prioritizing deployments in this way will maximize the security benefit that can be achieved with limited departmental funds and ensure that CBP has the capacity to compile, assess, and integrate the additional scan data into its effective, functioning risk-based strategy.

Lessons Learned Summary

The SFI pilots have benefited from host nation officials and port operators willing to expend, to varying degrees, the resources associated with additional staffing, alarm response protocols, construction and other infrastructure upgrades. Our foreign partners have also worked constructively with CBP and DOE/NNSA to resolve data sharing, health and safety, and other operational difficulties that arise. These partnerships with the international community and the private sector were critical to the initial SFI pilots and remain a key factor as DHS considers expansion of the program to higher risk trade corridors.

That said, global reactions to the mandate of the 9/11 Act have been significant. In several unedited appendices to this report, SFI foreign government partners (Appendix A), SFI terminal operators (Appendix B), trade and industry groups (Appendices C and D), and other foreign governments (Appendix D) have submitted reports, correspondence, and/or reviews of the “100 percent scanning” policy. Many express concerns that this policy will negatively impact container processing, increase operating costs, infringe on state sovereignty, and unnecessarily burden security organizations. As partnerships with host nation governments and terminal operators are at the center of every successful SFI/ICS deployment, our continued partnerships with them to address these legitimate concerns are indispensable.

Foreign partners are not consistent in their commitments to expend resources on the SFI pilot and to continue SFI operations when the pilot concludes. Different countries’ legislation, limited resources, and other national concerns contribute to the different approaches.

For example, the United Kingdom is a strong partner in implementing multiple security programs to help protect the supply chain, and Her Majesty’s Revenue and Customs (HMRC) was one of the first foreign customs services to participate in SFI. The scanning

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

system in Southampton pilots some of the latest technology and has yielded valuable results in testing the integration and scanning capabilities of these systems. Despite solid cooperation, obstacles remain and in Southampton transshipped containers proved not only logistically difficult to scan, but sharing the data on them proved legally difficult – two separate obstacles requiring two solutions.

Transshipped containers pose a logistical difficulty because, unlike traffic passing through the terminal gates, these containers do not pass through the SFI scanning systems. Developing a process to scan transshipped cargo was the first obstacle. While CBP and DOE preferred U.S. bound transshipment containers to drive through the SFI system, Southampton Container Terminal (SCT) believed that this approach would hinder their operations. Therefore, as a compromise, HMRC, CBP, DOE, and SCT developed a solution in which all U.S. bound transshipped containers are scanned for radiation by U.S. personnel using handheld detection equipment. However, this solution led to a second obstacle: according to HMRC, U.K. privacy laws do not allow the British government to share image data with the United States, unless there is a risk associated with the container (i.e. a radiation alarm). Under the transshipment process, the SFI team is dependent on HMRC equipment to take the NII image of transshipped containers. A compromise was reached in which, using its own equipment, HMRC has agreed to take images of all transshipped containers that show signs of radiation, and share the data with U.S. personnel in Southampton. This process began on March 3, 2008. The situation within the United Kingdom highlights the fact that even if the physical logistics of an obstacle, like transshipment, can be overcome, legal or other national concerns make overall practical solutions difficult.

Another example of the need for partnerships with the international community is the condition expressed by some foreign government partners that this pilot not last longer than six-months. The Singapore government has requested that all equipment be removed at the end of the SFI pilot phase, despite the 100% scanning mandate established by the 9/11 Act. To facilitate that request in a cost-effective manner, CBP agreed to procure mobile systems, which can be easily removed after the pilot. DOE also agreed to modify its standard design for radiation detection equipment installation in order to create a solution that could be installed and then removed and relocated after six months in a cost-effective manner.

HMRC has also limited their participation in the SFI program after completion of the pilot on April 12, 2008. HMRC chose not to staff the SFI site in Southampton after April and has reverted back to CSI protocols (agreed to in 2002). The United States government has been considering alternative solutions to continue operations.

The initial SFI pilots have demonstrated that technical and operation solutions are not yet available to capture transshipped cargo efficiently. New equipment and software must be developed to address the considerable challenge of scanning containers that often transit through ports quickly and without necessarily being placed on trucks or passing through port gates. To date, SFI has progressed on a limited scale in ports that take advantage of the natural chokepoints of entry and exit gates to scan containers. This approach

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

typically prevents significant impact on port operations, but is not applicable in heavy transshipment ports where containers arrive on one ship and depart on another without entering or exiting through the port gates. Because of shorter dwell times for containers, space constraints, lack of immediate availability of shipping data, and the difficulty of identifying chokepoints within busy container terminals, capturing transshipped cargo without seriously impacting port operations remains a significant challenge. Solutions to this challenge will depend upon the specific infrastructure conditions at any given port, technology interface issues, and the development of operational procedures in concert with host nation and port officials. Advances in technology that require a smaller physical footprint are also essential to any future implementation of SFI.

Discussions with the port of Singapore have highlighted the fact that developing and executing a concept of operations in a higher-volume/transshipment port will prove to be more challenging than in ports that process mainly gate traffic. The port of Singapore has very short dwell times that require extremely efficient processing of containers. As documented in the Government of Singapore's report (see Appendix A), Singapore projections indicate that SFI will have a detrimental effect on the processing times in the port. Although no such effect has been seen in the initial three SFI pilot ports, these locations do not process a large amount of transshipped cargo and the expectation is not unreasonable that transshipment operations, such as those in the port of Singapore, have the potential to create inefficiencies and will pose a challenge.

While highlighting many challenges, the SFI pilots have also produced valuable and positive feedback. SFI, in the initial three ports, has demonstrated the operational feasibility of integrating various scanning technologies and transmitting data in near-real time for review and analysis. SFI has also demonstrated that scanning data associated with maritime containers at a port of lading can be integrated into CBP's ATS and reviewed alongside the targeting system's risk assessment rule sets. This information can be successfully integrated by electronically linking specific container identification data to that container's scanning data. To date, CBP has successfully integrated, transmitted, and received thousands of data files from the three operational ports.

Additionally, a preliminary analysis of the potential trade facilitation benefits of SFI has been positive. Containers arriving in the United States accompanied by SFI data do not experience the same rate of examination at U.S. ports as containers that originate from non-SFI locations. As well, the additional data elements gathered at the foreign port assist CBP officers in more quickly and efficiently mitigating risk and adjudicating radiation alarms occurring at a domestic seaport.

The initial deployments under SFI also demonstrate the significant costs associated with procuring and deploying scanning technology and the supporting information technology (IT) infrastructure. With the announcement of SFI in 2006, DHS and DOE each committed approximately \$30 million toward the implementation of SFI in the initial three ports and toward the deployment of additions and systems at three of the limited capacity pilots. The following table details the total cost incurred by DHS and DOE in establishing SFI in FY 2007 at the three 100 percent scanning ports and preparing for

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

deployment to the limited capacity ports. The chart does not include costs associated with the deployment of the additional CBP personnel initially required to set up the integrated scanning systems and augment the in-country CSI teams or any out-year costs associated with annual communication and IT or equipment operation and maintenance.

Table 1-1 DHS and DOE Costs

DHS Cost Element		DOE Cost Element	
Analytical Study	\$ 200,000	Equipment	\$ 5,046,757
Communications	\$ 2,709,879	Installation	\$ 15,365,581
Equipment	\$ 10,155,000	Testing	\$ 465,000
Hardware	\$ 2,996,194	Maintenance	\$ 550,000
Hardware (server license)	\$ 82,132	Communications	\$ 5,935,582
Port Deployment Support	\$ 463,923		
Program Office Support	\$ 1,657,500		
Software Development	\$ 10,080,884		
Software License	\$ 628,486		
Software Support	\$ 140,535		
Training	\$ 231,502		\$ 1,913,000
Travel	\$ 1,099,093		\$ 106,687
DHS Total	\$ 30,445,127	DOE Total	\$ 29,382,607

Costs to industry and foreign partners were minimized during the initial SFI pilot by the use of primarily U.S.-owned systems in SFI ports, as well as U.S.-funded upgrades to terminal operating systems (TOS) and enhancing the local IT infrastructure. In addition to costs incurred by the U.S. Government associated with SFI scanning, the terminal operators are also absorbing costs in the form of fuel for the trucks, time to run containers through the systems, and utilities. With the exception of Puerto Cortes, terminal operators do not presently assess a fee to recoup their costs; however, they may begin to do this after the pilot phase. Additionally, our foreign Customs partners are absorbing costs associated with increased staffing levels including overtime, training, and personnel assigned to full-time operations.

Although DHS and DOE funded the initial phase of SFI deployments, the equipment, IT, and personnel costs associated with expanding the program to cover all U.S. bound traffic from the more than 700 different ports that ship to the United States – many significantly larger and more complex than any of the first three pilots – means that the benefit of immediate widespread deployments must be weighed against the Department’s funding needs to address other homeland security vulnerabilities. While RPM spectra and NII images can be useful additional data points for evaluating the risk of U.S.-bound containers, the constraints of existing budgetary restrictions and lack of universal solutions to make scanning cost-effective and efficient in every port underlies the Department’s strategy to focus future SFI deployments on trade corridors that present the

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

highest risk. Gathering scan data from these high risk corridors will provide additional information, consistent with the Department's successful layered strategy, for CBP targeters, enhancing risk assessments in the most vulnerable areas, without overwhelming the Department's budget, personnel resources, and ability to defeat other serious threats to the homeland.

As discussed above, the deployment of container scanning equipment at each of the SFI ports has presented certain operational, technical, logistical, financial, and diplomatic challenges that will likely continue to be encountered, to varying degrees, as SFI expands. These challenges include:

- Sustainability of the scanning equipment in extreme weather conditions and certain port environments;
- Varying costs of transferring the data back to the United States (National Targeting Center) in real-time, etc.;
- Re-configuring port layouts to accommodate the equipment without affecting port efficiency;
- Developing local response protocols for adjudicating alarms;
- Addressing health and safety concerns of host governments and respective trucking and labor unions;
- Identifying who will incur the costs for operating and maintaining the scanning equipment;
- Acquiring necessary trade data prior to processing containers through the SFI system;
- Addressing data privacy concerns in regards to the scanning data;
- Concluding agreements with partnering nations and terminal operators to document roles and responsibilities regarding issues such as: ownership, operation, and maintenance of the equipment; sharing of information; and import duty and tax considerations;
- Staffing implications for both the foreign customs service and terminal operator;
- Licensing requirements for the scanning technology;
- Reaching agreement with foreign and industry partners to continue scanning 100 percent of U.S.-bound containers after the pilot ends; and
- Discussing the potential requirements for reciprocal scanning of U.S. exports.

Each of the seven ports presented a unique set of challenges that required SFI managers to respond with a wide array of operational, technical, logistical, and diplomatic solutions. This report details the variety of challenges that arose as CBP and DOE/NNSA worked to implement the SFI scanning program in specific locations within a legislatively mandated timeframe. Significantly, the means by which certain issues were addressed in some locations were not necessarily available or appropriate in other locations. Each port will present its own unique set of challenges.

One example of a challenge requiring different solutions in each location was the different level of automation, with paper-based rather than computerized systems, in some of the initial SFI ports. In many situations, containers can arrive at the port up to several days before they are loaded on vessels. If containers arrive more than one day before lading, then CBP will not yet have the container's corresponding trade information, received under the 24-Hour Rule. Without information about what is in the container or whether it is U.S.-bound, resolving an RPM alarm or image anomaly is more difficult. CBP addressed this challenge in a variety of ways, including agreements with customs partners, terminal operators, and carriers for access to certain information (such as destination and commodity descriptions to identify U.S.-bound containers) that assisted with the risk assessment process and adjudication of radiation alarms. Those ports that lack an automated system will provide additional challenges for providing manifest and destination information to CBP.

The pilots have demonstrated that not just scanning equipment but a combination of technology, processes, and collaboration is necessary to a successful scanning system; additional necessary factors include innovative solutions to operational hurdles, useful data that is collected, analyzed and primed to enhance targeting, a collaborative approach with the international community and port operators, and perhaps most importantly, responsible and practical policies informed by the totality of the threats to which the U.S. remains vulnerable.

Central Alarm Station (CAS) and ATS Software

DOE has developed and deployed Central Alarms Stations (CAS) in 12 seaports under the Second Line of Defense (SLD) Program's Megaports Initiative, and is currently in the testing, development or planning stages in 19 additional seaports. A CAS is also deployed at SFI ports. The SLD CAS, consisting of hardware and software, collects data from RPM, cameras, OCR equipment, and other detection equipment, such as handhelds, and displays it in way that assist CAS operators in making decisions on alarming containers.

DOE contributed its CAS technology to the SFI partnership with CBP. Under SFI, DOE augmented its Megaports CAS by integrating new components, including an Advanced Spectroscopic Portal, and a Non-Intrusive Inspection system. One of the challenges of SFI was to package this information and deliver it for use by CBP. DOE worked closely with CBP to ensure that the data was collected and transmitted by the CAS in a manner that CBP could populate its data tables and merge it with the with data already existing in

CBP's ATS system. DOE and CBP convened a joint working group to develop the N.25 format, which wrapped all data associated with an occupancy, which ATS could unpack and repackage for its integrated viewer.

Like the Megaports standard CAS, the SFI CAS system also includes software that provides the analytical tools to enable CBP officers to resolve alarming containers. In addition to screening equipment, many SFI CAS, such as that Southampton, include integration with systems belonging to the terminal operators, to ensure that the terminal is aware of alarming containers and places holds in its system so that these containers are not loaded onto a vessel prior to disposition. In addition, SFI installations also include a CBP CAS, which is a window that allows CSI personnel stationed at the foreign port to see the same data that the foreign Customs CAS operators see.

CBP, in turn, has developed a software system, called ATS-SFI, which receives and re-packages the data sent by the CAS to CBP personnel with access to the ATS systems. This repackaged data is sent with the additional ATS-SFI data to the CBP personnel at the CBP CAS at the foreign port. The development of the ATS-SFI system has progressed well and has provided CBP officers with an unprecedented ability to view SFI scan data and corresponding trade information within a single computer system. Specifically, ATS-SFI has the capability to associate SFI data with other information used by CBP to assess each U.S.-bound shipment for risk, including targeting rule sets predicated on the advanced electronic cargo information required by the Trade Act of 2002 (including the 24-Hour Rule).

While the ATS-SFI software that integrates data elements produced by the scanning equipment represents a significant accomplishment, the full benefits of this capability cannot be realized without trained personnel (on-hand either domestically or abroad) to assess the collected data and address concerns identified by the integrated scanning system. CBP is aware of technological innovations, such as automatic anomaly detection capabilities, that may potentially aid in the assessment of these data points in the future. However, until that time, the human factor will remain an essential component of the analysis process and of the SFI/ICS system as a whole.

Effectiveness of Systems to Detect Shielded and Unshielded Nuclear and Radiological Material

The integrated scanning system consists of three components: the RPM; the radiation isotope identification device (RIID); and the NII scanner. The RPM and RIID provide the capability to detect and identify nuclear and radiological materials, while the NII captures either an X-ray or gamma ray image of the shipping container and its contents that indicates density.

The SFI pilots have thus far demonstrated that, when used together as an integrated system, these components have the potential to complement each other either by adding new functions to the detection capability or by refining the results generated by the other components. The equipment is capable of detecting special nuclear material (SNM) and naturally occurring radioactive material (NORM).

Each of the three detection components of the integrated scanning system performs different but complementary functions of the detection task. Each of the components has specifications relative to its applied functionality and has been tested and found to meet or exceed those specifications. The combined effectiveness of the three components is not measurable in the same manner as the effectiveness of the individual components. Testing has not been performed on the integrated scanning system as a whole; a more comprehensive assessment of its performance as implemented in the field will be based on the analysis of operational data collected over a longer period of performance and across a broader scale of deployment than those of the limited scope of the pilot program. System modeling and testing may also be necessary to fully assess integrated system performance.

Next Generation Scanning Systems

The development and integration of new technologies is critical to enhancing security without impeding commerce. As a force multiplier, technology can enable CBP to organize and sift through vast amount of data at critical nodes of the supply chain and provides CBP officers with the necessary information to apply preventive measures and reduce vulnerabilities. The use and ongoing development of radiation and nuclear detection as well as NII equipment provide examples of advancements in technology that could augment security dramatically. These scanning technologies promise to be important as we work together with the international community to increase radiation and nuclear scanning and enhance global supply chain security. However, technological improvements to next generation radiation detection and imaging equipment will be necessary to move forward with the implementation of the SFI program in an efficient and effective manner.

For NII imaging systems, software able to accurately identify high-risk anomalies in the image is being developed but is not technically mature. In collaboration with the Domestic Nuclear Detection Office (DNDO), efforts are underway to develop, integrate, and test image anomaly detection capabilities for integration into the SFI scanning system. Images currently require a trained officer to evaluate them. CBP and DNDO intend to continue to work closely together to improve anomaly identification software.

The hardware and software of next generation RPMs (e.g., Advanced Spectroscopic Portal (ASP) Monitors) are capable of discriminating isotopes of interest in shipments from radioactive material, including NORM. Because these next generation units have larger detectors than those in existing hand-held equipment and rely less on operator proficiency, they are expected to offer an advantage in the conduct of secondary scans. However, these units are significantly more expensive than the technologies currently being used. Additionally, it has not yet been established to what extent NORM isotopes may mask the presence of SNM; testing in this area is underway. Depending on the results of this testing and for certain applications where there is a significant amount of NORM traffic, these monitors may offer a useful alternative to current systems, in which isotopes in alarming containers can only be identified in the secondary scan. It should be noted that NORM masking is an issue for all spectroscopic systems, not just ASP. In

addition, use of these monitors as more powerful secondary inspection tools is currently being evaluated as a pilot program as part of SFI. The operational benefits of these monitors are still being evaluated.

SFI Expansion to Other Ports (Recommendations)

The implementation of SFI in Pakistan, Honduras, and the United Kingdom, and the limited testing in the four other SFI locations illustrates that the scanning of all U.S.-bound maritime containers in a foreign port is possible on a contained scale. While implementation at these initial ports has illustrated the considerable challenges and costs associated with scanning abroad, the additional data points obtained from the radiation scan and the radiography image have the potential to enhance the robust layers and effective risk-management principles already in place to secure the supply chain and may potentially represent a means by which integrated technologies and cooperative partnerships could enhance security without impeding commerce.

Section 231 of the SAFE Port Act requires this report to evaluate the pilots as well as the need and feasibility of expanding SFI/ICS. As DHS develops a specific policy forward, in conjunction with the DOE and the DOS, we will prioritize our resources and efforts by focusing on specific higher risk trade corridors where the most security benefit can be realized. Based on preliminary results from the three pilot locations, and in light of the considerable costs and challenges associated with the deployment of SFI/ICS systems, this high risk trade corridor approach accords with the current risk-based strategy, best addresses the greatest threats to the United States, and represents the most worthwhile investment of limited available resources for the scanning of cargo containers at foreign ports.

Considering the immense flow of containerized cargo entering the United States on an annual basis (11.5 million containers), as well as the interdependence of our nation's security and economic health, it is imperative that resources remain focused on ensuring the security of global commerce without interrupting the flow of legitimate goods. DHS has made steady progress and has dedicated significant resources to our cargo and port security programs over the last several years. These efforts have resulted in a robust risk oriented and layered approach to security that is based on informed judgment about the totality of risks we face from potentially dangerous goods and people entering our nation.

The issue of container security has precipitated much discussion and effort over the last several years, but the Department has also been, and must remain, attuned to other threats to U.S. ports and other potentially vulnerable components of the supply chain. Because maritime containerized traffic is not the only compelling threat area or vulnerability in need of resources, DHS has created a robust layered, risk-based strategy to ensure the integrity of the supply chain and the security of our Nation's ports.

While evaluating the need and feasibility of expanding SFI/ICS, this report also includes additional information that addresses the following eight subsection requirements of the SAFE Port Act (Sec 231(d)(5)(a) through (h)).

Infrastructure Requirements

As this report discusses, each port may share basic infrastructure requirements, such as specific equipment, minimum port requirements, and information technology/communication systems, but each port is also unique, based on issues like the layout and quality of the infrastructure, environmental and weather factors, space constraints, etc. This means that actual operational solutions to challenges encountered deploying SFI scanning equipment vary greatly from port to port.

For example, each port will require radiation detection and imaging equipment as well as the physical space, or footprint, upon which to operate these technologies. The NII equipment poses a particular challenge as it requires a minimum distance from the RPMs, so as not to impact RPM operation, and an exclusion zone for safety considerations. Furthermore, an enhanced IT infrastructure is needed to push the SFI scan data to CBP officers located both the foreign port and in the United States. This often requires software modification to the equipment and to the terminal operators' systems.

Processing Speeds of Containers

The initial SFI pilots have demonstrated that the average speed in which a container is processed through the SFI/ICS equipment is three to five minutes. This three to five minute period includes the time required by a CBP Officer to analyze the image to determine whether additional scrutiny is required. Those containers that require further inspection with a radiation handheld device are delayed for an additional five to ten minutes. Appendices C and D of this report provide feedback from the trade on the SFI pilot and note that the delays and bottle-necks expected in these initial locations did not materialize. Additionally, dwell times at the three operational SFI ports are currently relatively long (measured in days, rather than in hours or less, as is the case in some larger ports) which helped to ensure that processing through the scanning systems did not cause any container to miss its voyage. While this speedy processing of containers is beneficial, it remains important to note that supportive features present at the initial three SFI pilot ports, such as the relatively low-volume, lower dwell times, and lack of significant amounts of transshipped cargo, are not characteristic of all ports.

Scalability of the Systems to Meet Current and Future Trade Flows

From a basic equipment and resource allocation perspective, scaling the capacity of the SFI integrated scanning system is a matter of installing sufficient amounts of equipment and appropriate system capacities to manage peak container traffic volumes without negatively impacting port operations and causing shipping delays. Without constraints and excluding the unique challenges associated with transshipped cargo, the current system could be scaled to address any container processing volume. However, the constraints of available space, the number of assigned personnel, the limits of host government cooperation and the realities of the considerable costs associated with the procurement, installation, operation, and staffing required to review and analyze the data and respond to potential alarms, establish a practical limit to the amount of container traffic that feasibly can be processed in an efficient manner through the system.

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

Furthermore, due to health and safety concerns, many foreign government regulations prohibit the use of drive-through imaging systems, which are necessary to ensure the efficient processing of containers.

Cataloging Data for Reference and Analysis in the Event of a Transportation Disruption

If a transportation disruption resulted from the actual use or forecasted use of a container for terrorist purposes, data and images gathered by the SFI/ICS could play a significant role in resumption of normal trade for containers originating from SFI ports, offering additional data points that could be used with the other risk-assessment tools that are part of DHS's existing layered strategy. The images and associated data of containers that are scanned and cleared by CBP at an SFI port would be reviewed alongside ATS risk assessment rule sets and situational intelligence to provide CBP officers with enhanced information when determining the level of risk associated with each container. This would allow CBP officers to make informed decisions when identifying high-risk containers, while facilitating the release of containers categorized as low-risk.

Requirements for Installation and Maintenance of the Integrated Scanning Systems

The key requirements for installing an integrated scanning system are: the cooperation of the host country government and port or terminal management; addressing the health and safety concerns associated with imaging systems; procuring the integrated suite of scanning equipment including RPM, RIID, NII, License Plate Reader (LPR), and OCR devices; the physical space necessary for equipment installation; sufficient additional space to allow the establishment of container traffic flow through the scanning system and for performing secondary inspections; acquiring necessary manifest and destination information prior to processing containers through the SFI system; and the financial resources to accomplish the installation and operation.

Secondary requirements include the computing systems and software necessary to collect, store, and evaluate scanning results; local network cabling to interconnect scanning devices and computing systems; facilities to house computing systems and personnel; and communications circuits to enable data transmission to the CBP National Data Center (NDC). Construction is required for any infrastructure upgrades that may be necessary to facilities and roadways at the port or terminal and for strengthened foundations for permanently installed NII, RPM, and OCR equipment. As noted in the chart above, in Fiscal Year (FY) 2007 DHS and DOE spent almost \$60 million to install scanning systems in the three initial SFI ports, and for preliminary efforts to set-up systems in four additional ports. This amount does not include future costs associated with continued data transportation or equipment maintenance and upgrades.

Staff is also required to support the operation of the SFI/ICS by adjudicating radiation alarms. The system is required to be operational during those hours when container traffic is entering the port. In most ports, this requires staff to be on duty 24 hours per day, either six or seven days per week. Depending upon the port, operations staff may be CBP personnel, Foreign Service Nationals (FSN), Terminal Operators or foreign customs

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

personnel. Once available, CBP staff then review and analyze the integrated radiation and radiography data in conjunction with the 24-Hour Rule information and any other available information to determine whether to clear a container for loading or request further examination. Only host government personnel, usually customs or law enforcement, have the authority to perform examinations.

Ability of the Staff to Use Scanning Data

Operations in the pilot ports have demonstrated that data captured by the three components of the scanning process, to include NII images, radiation detection profiles, and container identification information, can be efficiently and effectively integrated and provided to CBP officers who have access to ATS and other CBP systems through a single, consolidated viewer. CBP officers in a variety of roles have the ability to view and analyze container images and associated data captured to examine high-risk containers without having to compile data from multiple, separate computer systems or consult separate automated or non-automated data repositories. Data are accessible by CBP officers stationed at SFI ports, CBP targeters on duty at the National Targeting Center- Cargo (NTC-C), Laboratories and Scientific Services (LSS) personnel who may be consulted on the assessment of a container, and by CBP officers on duty at domestic ports.

Some of the factors discussed in this report that impact a CBP officer's ability to best use the scanning data obtained through SFI/ICS include: the availability of commercial data at the point when a container enters the port, possible foreign government restrictions against sharing data with U.S. personnel, and the level of automation of a specific port. CBP and DNDO have been working closely on new decision-support tools as part of the consolidated viewer, including the NII image anomaly algorithms for pilot testing. Currently, however, NII equipment, (to include X-ray and gamma ray systems) has no automated alarm capability and the images generated by these systems require human interpretation and evaluation to determine whether the image reflects an anomaly or is consistent with manifested goods. A CBP officer reviews the NII image carefully before determining whether the container can proceed or is subject to further inspection. The time required for this process of review and analysis is difficult to calculate precisely, but will remain a critical component of the process until this equipment has the capability to rely upon fully automated processes to help identify potential shielding material. This necessary review and analysis of scan data by trained USG operators presents a significant challenge to the expansion of the program to port locations that process higher volumes of containers.

Ability to Safeguard Commercial Data

CBP has extensive experience using commercial data when conducting its risk assessments. CBP has been working closely with the maritime industry for many years, routinely interacting with the DHS Commercial Operations Advisory Committee (COAC), the Trade Support Network (TSN), and other trade organizations to establish guidelines for using sensitive trade data. At the SFI pilot ports, a software application

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

developed by DOE collects non-commercial device data about shipping containers from multiple sources – the RPM, the radiographic imaging equipment (NII), and an OCR that records the shipping container number. Data from each source is transferred to the CAS via individual direct ethernet connections. Each data stream contains only the data from the scanning device and does not include any commercial information. Physical security and maintenance of the CAS is the responsibility of the host country.

At each SFI location, a U.S. Government-owned-and-maintained network router provides firewall protection for the dedicated network connections from the SFI pilot port to domestic CBP systems. Additionally, the router encrypts the data collected by the CAS and transmits it through the firewall to the NDC. Once the CAS data is securely behind the NDC firewall, it is integrated with the commercial data provided in compliance with the 24-Hour Rule.

The Reliability of Currently Available Technology

To be considered reliable, the SFI integrated scanning system must function in the environment where it is installed, exhibit the capacity to process workloads encountered, and require minimal downtime. Not unexpectedly, and as discussed later in the report, NII systems and RPMs deployed to the initial SFI ports have experienced service outages and failures requiring repair. Where redundant elements are included in the system design (such as in the port of Qasim, Pakistan), full operations are able to continue while repairs are made. If there is no redundancy for the failing component, that portion of the scanning process does not occur. While individual components of the integrated system may experience service outages or failures requiring repair or replacement, the impact on the overall integrated scanning operation can be reduced if each installed system includes some level of component redundancy or if operational alternatives are developed so that overall system operation and integrity are not compromised by a single component failure. Note that procuring redundant equipment also increases the cost of the SFI operation.

DOE and CBP have acquired RPMs and NIIs from a number of manufacturers and have developed standard performance and reliability specifications for inclusion in procurement requests. Some of the details from these specifications for RPMs and NIIs are listed below. The complete performance specifications can be found in Section 5(H) of this report.

RPM Reliability and Performance Specifications:

DOE currently deploys RPMs in primary detection that use plastic scintillation and Helium-3 (^3He) tube technology. Prior to the selection of its current RPM vendor, DOE issued a Request for Proposal (RFP) containing the specifications that rail and vehicle RPMs and their associated communications systems must meet. The criteria listed below were part of that specification. Additional performance and reliability specification criteria for the RPMs and the associated communications equipment can be found in Section 5(H).

Monitor Specifications:

- Gamma detectors must be large plastic scintillators.
- To detect the presence of shielded plutonium the monitor must have moderated ^3He detectors.
- The monitor must be capable of determining and indicating separate neutron and gamma alarms.
- The monitor must be specifically designed to detect the low energy gamma rays characteristic to weapons grade highly enriched uranium (HEU) and plutonium.
- The monitor must be equipped with battery back-up capability that allows it to operate at least 12 hours without external electrical power.

NII Reliability Specifications

- System should have a minimal footprint.
- Penetration of a minimum of 300 mm of steel.
- Minimum source strength not less than 6 MeV for portal system and 3.8 MeV for mobile system.
- Resolution requirements shall be .125 inches, preferred, but not less than .5 inches.
- Capable of continuous operation for 24 hours per day, 7 days per week.
- Have low dose rate emissions per inspection.
- Capability to scan 20-48 foot chassis-mounted sea containers in one pass.
- Scan a minimum of 75 containers per hour and, preferably, up to 150 containers per hour for portal type systems. Mobile units must be able to scan a minimum of 30 containers per hour.
- Transmit images to a designated location in the United States via the N-25 format (N-25 baseline version 1.4) and be N-25 compliant.
- Operate as an automated drive-through system for both partial and mobile units.
- Measurement and imaging of containers/vehicles is independent of direction of vehicle motion.
- Must be integrated with redundant safety features.
- Must provide for radiation safety of operators, workers, stevedores and bystanders while maintaining a minimum footprint.
- Ability to operate effectively in extreme temperatures and accommodate worldwide deployment conditions.
- Ability to operate on universally accepted power standards.
- Must be compliant with all safety and certifications requirements in the country in which its deployed.
- Workstation and Interface System must include an Operator Console and all operating systems, software, cameras, controls and displays to depict a video and radiographic image of the target.
- Capable of capturing and displaying the radiographic and visible spectrum (video) images of the target to the Operator simultaneously.

Background

The priority mission of CBP is to enforce the laws of the United States at our borders while facilitating legitimate trade and travel. To accomplish this goal, CBP relies upon on a layered risk-management approach that identifies and stops threats without impeding commerce and endangering the economy of the country. DHS has put into place multiple levels of security mechanisms to ensure the integrity of the supply chain. 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.

Using information to accurately assess risk is at the heart of our layered strategy to securing cargo as it transits the international supply chain and our goal is to combine existing systems, programs, and capabilities to allow us to receive, process, and act upon commercial and security information quickly and efficiently, thus mitigating threats with the least possible disruption to legitimate trade.

The use of advanced trade data and automated targeting capabilities to assess the risk of every shipment entering the United States not only allows us to focus our resources on the real threats, but it helps us recognize lawful shipments, thereby reducing the burden of unnecessary inspections and promoting the speedy flow of legitimate trade. The 24-Hour Rule and the Security Filing proposal (“10+2 initiative”) focus on obtaining advance electronic information on cargo and human players throughout the supply chain. Our automated systems analyze this data, assessing each U.S.-bound shipment for risk, and our CBP officers stationed at home and at foreign CSI or SFI ports evaluate each container and ensure, using technology or physical means, that concerns related to all high risk cargo are addressed.

Peer reviews and other enhancements continue to strengthen the ATS, one of the fundamental decision support tools available to CBP officers working in Advance Targeting Units (ATUs) at ports of entry and CSI ports. The system provides a uniform review of cargo shipments, identifies the highest threat shipments, and presents data in a comprehensive, flexible format to address specific intelligence threats and trends. ATS uses a rules-based program to highlight potential risk, patterns, and targets which alert the user to data that meets or exceeds certain predefined criteria.

Additionally, the importer and carrier Security Filing proposal (“10+2”), published in the Federal Register on January 2, 2008, will allow CBP to obtain additional advanced cargo information and enhance our ability to perform risk-based targeting prior to cargo being laden on a vessel overseas. Increasing the information we get on shipments enhances our ability to target true threats and reduces the need for costly and time-prohibitive physical inspections of legitimate goods. Comments received under the notice of proposed rulemaking for this proposal, which closed on (March 18, 2008), are currently under review by CBP.

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

Strong partnerships with the trade and foreign governments, such as through C-TPAT and CSI, offer additional layers of security, which enable CBP to enhance security in parts of the supply chain beyond our borders. Under C-TPAT, CBP works in partnership with the trade community to better secure goods moving through the international supply chain. C-TPAT has enabled CBP to leverage supply chain security throughout international locations where CBP has no regulatory reach. In FY 2009, C-TPAT will focus on strengthening the partnership with member companies at both the macro and micro levels and leverage corporate influence throughout the international supply chain. In doing so, C-TPAT will continue to ensure compliance with the requirements of the SAFE Ports Act to include certifying security profiles within 90 days of submission and conducting validations within one year of certification and revalidations within three-years of the initial validation. C-TPAT projects that 3,800-4,500 validations will be required during FY09, requiring onsite visits at facilities throughout the world.

In strengthening this successful program, CBP will also continue to review its performance and, where needed, enhance the minimum security criteria for each enrollment sector. Additionally, CBP will continue to conduct informational and training sessions for various internal / external audiences to improve knowledge of cargo security procedures and provide the latest information regarding terrorism trends and conveyance breaches.

Another established and successful layer is the CSI program, which helps CBP meet the priority mission of preventing terrorists and terrorist weapons from entering the United States. Under CSI, the first program of its kind, CBP partners with foreign governments (currently at 58 foreign ports) to identify and inspect high-risk cargo containers before they are shipped to our seaports and are in a position to pose a threat to the United States and to global trade.

An additional part of CBP's comprehensive strategy to combat nuclear and radiological terrorism is to scan all arriving sea containers with radiation detection equipment once they arrive in U.S. ports and prior to their release into the U.S. economy. Currently, CBP has 398 RPMs deployed at priority seaports in the United States, through which approximately 98% of all arriving sea-borne containerized cargo passes. CBP, with the Domestic Nuclear Detection Office (DNDO) and DOE, is also working to test the next generation of radiation detection equipment.

These programs form the backbone of CBP's risk-management, layered enforcement strategy. To most effectively manage the risk to our country, we must direct our resources to those areas which represent the greatest threat. We are constantly working to refine this layered process; our efforts focus on strengthening our tools and capabilities while at the same time maintaining an appropriate balance that considers the wide range of threats and allocates our limited resources accordingly.

Comparison of the CSI, Megaports Initiative (MI), and the SFI International Container Security Pilots

CSI Approach

CSI was announced in January 2002. Initially implemented at the 20 ports that ship the greatest volume of maritime containerized cargo to the United States, CSI has since expanded to additional seaports of economic and strategic significance and is currently operational at 58 ports worldwide.

CSI's true value is the relationships CBP officers develop with their CSI host nation counterparts. The knowledge and specific expertise of host nation officials leads to valuable additional country-specific and local information that validate, enhances or negates the risk associated with shipment entities, addresses, and commodities, improving the CSI team's ability to resolve anomalies and assess threats during their review of U.S.-bound containers. Better information enhances our ability to identify true threats and focus our resources on these, but it also helps resolve anomalies on legitimate traffic, removing concerns that could lead to unnecessary delays, allowing it to progress to its destination.

CSI personnel, working in partnership with host nation government officials, screen 100 percent of U.S.-bound maritime cargo laden at CSI ports and perform risk-based targeting on shipping manifest and bill-of-lading information associated with particular shipments. When a high-risk shipment is identified through ATS, it is further analyzed by CSI officers. These officers can refer a suspect container to host-country customs officials for examination, which may include radiation and NII imaging scans. If the scan data indicates a potential issue such as a radiation alarm or an image anomaly, CSI officers request that the host government perform further examinations of the container and its contents, in accordance with local laws and regulations. This process begins when CBP receives manifest information from the carrier, 24 hours prior to the container being laden on the departing vessel. The dwell time for the containers targeted by CSI ranges from hours to days, determining how much time CBP officers and host governments will have to act on high-risk containers.

Megaports Initiative Approach

The MI, established in 2003 as part of the Office of the Second Line of Defense, is an important nonproliferation program of the U.S. Department of Energy's (DOE) National Nuclear Security Administration (NNSA). The MI provides passive radiation detection equipment, communications systems, training, and technical support to international partners with the objective of enhancing their capability to deter, detect, and interdict the illicit trafficking of special nuclear and other radioactive materials through the global maritime system. Radiation detection equipment installed under this program looks for the presence of special nuclear and other radioactive materials in containerized cargo, alerting port and government officials of the need to examine the container and take appropriate action. These efforts help reduce the probability that materials could be used in a weapon of mass destruction or a radiological dispersal device against the United

States or its international partners. The goal of the MI is to scan as much container traffic at a port as possible (including imports, exports, and transshipment), regardless of destination. The MI uses a risk-based approach to guide implementation priorities, which uses both volume and regional threat to identify ports of interest.

Secure Freight Initiative Approach

As outlined above, DHS has in place a comprehensive policy to ensure that all cargo posing a risk to the United States is thoroughly addressed. The multiple tools in our layered approach revolve around gathering information and data relating to containers as they transit the global supply chain and the newest tool Secure Freight Initiative (SFI), builds on this concept. SFI includes the International Container Security pilots, which seek to gather RPM and NII scan data on containers in foreign ports and the Advanced Security Filing (known also as the “10+2” initiative), which expands the advanced commercial data that carriers and importers are required to submit to CBP. Although CBP continues to explore a third component of SFI called the Global Trade Exchange (GTX), aimed at organizing and integrating commercial and security information about shipments, no contracts were awarded in response to the recent solicitation for the trade data system.

Under the ICS portion of SFI, CBP uses an integrated network of radiation detection and container imaging equipment and data integration capabilities at overseas ports to gather additional information on maritime containers bound for the United States. These new sources of data are integrated into the CBP risk management process. Under the current SFI/ICS process, the timeframe for scanning containers typically precedes the filing of 24-Hour Rule information. Scanning occurs upon arrival at the port, prior to any risk assessment being conducted by ATS. Subsequent to scanning, a determination is made as to the need to perform additional examinations. Scan data are stored by CBP, fused with manifest information in ATS, and can be accessed at any point in the risk assessment process. The SFI pilot includes scenarios where targeting analysis is performed by CBP officers on location in the pilot ports and a scenario in which targeting is performed at the NTC-C in the United States, based on scanning data and images transmitted from the ports. The NTC-C targeting approach may in the future provide a means to reduce in-country staffing requirements.

Report Methodology

The DHS Secretary was directed to report to Congress on lessons learned from piloting integrated scanning systems under the SFI/ICS pilot study. This report is based upon data collected during initial negotiations, systems installations and initial testing, and full ICS pilot operations. Information was gathered through assessments, reviews, and interviews with CBP and DOE staff and contractors, host country officials, trade personnel, and terminal operators.

Discussion

An evaluation of the lessons derived from the pilot program

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

The integrated scanning systems pilot, implemented under Phase I of SFI, provided valuable lessons that will guide the expansion of the program. These lessons were drawn from experiences at the three SFI pilot ports in Puerto Cortés, Honduras; Port Qasim, Pakistan; and Port of Southampton, United Kingdom, where the goal was to scan 100 percent of U.S.-bound cargo. Additionally, the report also outlines lessons derived from initial USG efforts to deploy scanning equipment to four additional locations including Busan, Korea; Singapore; Port of Salalah, Oman; and Hong Kong. The goal in these additional ports is to deploy the integrated scanning equipment on a limited basis to better understand the challenges associated with implementing SFI in larger, more complex locations. This section will detail the progress made to-date in each of these locations.

FULL CAPACITY 100 PERCENT SCANNING PORTS

Southampton, United Kingdom

The SFI pilot at Southampton, United Kingdom, demonstrated successful integration of the technologies selected for the pilot operation. Implementation and operation of the SFI scanning process did not significantly impede the flow of container traffic through the port's container terminal, SCT, nor has it resulted in traffic bottlenecks within the terminal. SCT reports that concurrent with the installation, testing, and operation of the SFI pilot, container volume through the port increased to record levels with no resultant shipping delays, showing little or no negative effects of the pilot on the flow of container traffic through the port.

However, the pilot in Southampton was not without challenges, ranging from the realm of policy and negotiation, to the intricacies of technology, to environmental factors. The two most difficult problems encountered in Southampton were capturing transshipment containers and negotiating the post-pilot operation of the scanning equipment. U.S.-bound transshipped containers, which arrive at the port on one ship, remain inside the terminal and do not pass through the terminal gates on their way to being transferred to a U.S.-bound vessel. During the SFI installation planning process, SCT advised that rerouting transshipped containers back through the gates would have created a significant disruption to the speed and flow of traffic in the terminal, so an alternative process had to be developed. CBP and DOE worked with SCT to develop a compromise scanning process. All parties agreed that the SFI team would use hand held radiation detection equipment as a primary inspection tool to scan transshipped containers. While HMRC was able to provide NII scans from UK- owned equipment that was conveniently located to capture transshipped cargo, another challenge arose when HMRC informed CBP that U.K. privacy laws do not allow the British government to share image data with the United States unless there is a risk associated with the transshipped container (i.e., a radiation alarm). HMRC, CBP, and DOE recently reached a solution in which all transshipped containers are scanned for radiation, and HMRC images all containers that alarm for radiation using its equipment, and shares the data with U.S. personnel in Southampton. While this solution allows us to perform radiation detection on all the transshipped cargo, the legal impediment, combined with the financial and logistical necessity of using U.K.-owned imaging equipment to capture transshipments, prevents the

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

U.S. Government from receiving images of containers that do not alarm for radiation. So while we are getting good data on transshipments, this is a significant obstruction to reaching 100% integrated scanning. This process began on March 3, 2008.

The SFI pilot phase in Southampton ended on April 12, 2008. HMRC expressed its intent to cease participation in the SFI program after the pilot was complete, chose not to staff the SFI site in Southampton after April, and the process has therefore reverted back to CSI protocols (agreed to in 2002), with CBP Officers staffing the site. The United States government has been considering alternatives to continue operations.

Technical problems have also resulted in service outages of the NII imaging system installed at Southampton. This model is the first of its type installed by the vendor, and some operational and servicing issues were unresolved at installation time. The single NII device experienced outages and down time throughout the pilot program. Two major components of the NII machinery separately failed – the compressor, which required two days to repair, and the Betatron (the particle accelerator/transformer), which failed as a result of accumulating condensation during rainy conditions and required almost two weeks to replace.

Additionally, the U.S. Government was charged customs duties and Value Added Tax (VAT) by the U.K. government for both the equipment and construction of SFI in Southampton, amounting to approximately \$500,000 in additional expenses. CBP and DOE undertook lengthy negotiations to obtain a waiver. Eventually, CBP and DOE received temporary customs duties and VAT waivers for the duration of the pilot, which ended in April 2008. If, however, the pilot is extended, all customs duties and VAT will come due retroactively.

Another complication in Southampton was that CBP was informed of a requirement to comply with the United Kingdom Ionizing Radiation Regulations (IRR) of 1999, a U.K. health and safety law, only after negotiations, testing, and deployment of the SFI pilot were complete. To comply with this requirement, a Radiation Protection Advisor (RPA) was contracted to train and certify four on-site radiation security officers (RSO) to U.K. standards. To address concerns about potential health and safety risks of the scanning equipment, the SFI office proactively works with independent radiation authorities in several countries, including the radiation protection service for the United Kingdom Atomic Energy Authority.

Three final experiences bear noting. First, in the United Kingdom, the maximum height of trucks is nearly a foot higher than in the United States. Modifications to the NII portal – which was too short - were required to allow loaded U.K. trucks to pass through that device. Second, environmental regulations also had to be considered. In Southampton, the area next to the CAS installation contains a pond with a resident population of endangered turtles. Construction planning was modified to accommodate this situation. Finally, because many containers arrive at the port more than 24 hours in advance of their vessel's departure, CBP will not have received any corresponding commercial data (collected under the 24-Hour Rule). Therefore, CBP needed consent from the host

government and cooperation from the terminal operator to provide nominal information on a given container that was U.S.-bound (helpful for resolving radiation alarms on shipments containing material emitting naturally occurring radiation). However, the European Union places limits on the amount and type of shipping data that can be shared by member states with other governments. CBP and DOE worked with HMRC and SCT to agree that SCT would provide at least commodity and destination data to CBP for alarm adjudication.

Port Qasim, Pakistan

The SFI pilot at Port Qasim, Pakistan has demonstrated another successful integration of the technologies selected for the pilot operation. It showcases the successes of the SFI program in a country where the foreign government is very supportive of the initiative; from waiving the value added tax (VAT), to providing adequate staffing levels for SFI, the government of Pakistan has consistently proven to be a strong partner in piloting a system to scan 100 percent of U.S.-bound maritime containers.

Lessons learned from the Port Qasim pilot uncovered several important challenges that must be addressed, but also illustrated some trade benefits. A paramount concern is the downtime of the equipment used to scan the containers. Extreme climate conditions and lengthy operations times caused technological problems with the equipment that the vendors continue to address.

Port Qasim presented a unique situation since DOS does not allow U.S. personnel to be permanently stationed at the port for security reasons. As a result, all targeting of containers must be done remotely by CBP officers in the United States and physical exams at Port Qasim are conducted by Pakistan Customs officials and foreign service nationals (FSNs) hired by the U.S. Embassy. At all times, CBP Officers use live video feeds streaming directly from Pakistan to the United States to monitor SFI operations in Port Qasim. Creating the process for real-time data transmission and analysis required the development, installation, and integration of new software.

The trade is benefiting from SFI operations Port Qasim. In the time since SFI started operational testing, Port Qasim has experienced an increase in the container volume of exports to the United States. Shippers in the region are routing more containers bound for the United States through Port Qasim, in anticipation of faster processing through U.S. Customs upon arrival of containers that have been scanned at Port Qasim prior to shipping.

Puerto Cortés, Honduras

The selection of Puerto Cortés as an SFI pilot port provided an opportunity to pilot scanning equipment in a port with a higher volume of container throughput than at the other full-capacity pilot locations.

Several specific challenges proved obstacles to implementing SFI in Puerto Cortés. First, the terminal operator in Puerto Cortés has limited advance electronic data available and

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

containers may arrive days in advance of departure. Since manifest information is received by CBP only 24 hours in advance of departure, when containers arrive at the port gate days in advance and proceed through the scanning equipment, the manifest data has not yet been submitted to CBP or the port. The separation of U.S.-bound containers from non-U.S.-bound containers at Puerto Cortés occurs only after a manual documentation review by Honduran Customs personnel who are stationed at the scanning sites. This is later validated once CBP receives the 24-Hour Rule information.

A second challenge is that the NII equipment in Puerto Cortés was purchased separately by the government of Honduras and in advance of the development of integrated radiation scanning systems. There were difficulties integrating this older generation equipment with the radiation detection equipment used in the SFI pilot. For example, the imaging systems were initially unable to fuse some NII data with corresponding radiation scanning data, system reliability was adversely affected, and initially the overall data quality was poor.

Third, scanning equipment was not initially compatible with the N.25 standard used by CBP systems. This was due to the fact that implementation of DOE's Megaports Initiative at Puerto Cortés was already underway at the time of SFI selection. At the time Puerto Cortés was selected as an SFI pilot project, the system design including the software and database had already been completed under the Megaports Initiative. The scanning system was retrofitted with the N.25 standard, which caused temporary system reliability challenges.

Fourth, the labor union at the port voiced concerns about health and safety issues attributable to radiation exposure from the scanning equipment. A radiation safety fact sheet was provided by the U.S. Government on the safety of the equipment with documented, independent research on equipment safety.

Finally, CBP personnel can only work six days a week from 8 a.m. to 6 p.m. due to staffing safety concerns. Personal safety is a concern when traveling back and forth from the port to CBP housing due to the high crime rate along that route. When CBP staff is not present, any U.S.-bound container that triggers an RPM gamma alarm is sent to a holding area and handled by CBP officers when they return at the start of the next shift. For neutron alarms on U.S.-bound containers, immediate action is required. The Direccion Ejecutiva de Ingressos (DEI) will notify CBP officers, who will direct the next actions to be taken as they respond back to the port.

LIMITED-CAPACITY PORTS

Hong Kong

SFI in Hong Kong is the first of the four limited capacity ports to enter the operational testing phase. SFI systems are in place and testing the data and container flow to ensure optimal performance. These systems have been testing since November 19, 2007, and already have yielded valuable lessons. On January 11, 2008, limited scanning in Hong Kong became fully operational and is working well.

One of the most difficult challenges in Hong Kong is the limited space in which to place these systems. Jointly, the United States and Hong Kong Governments, as well as the Modern Terminal LTD (MTL), developed and implemented a CONOPS that fits this scenario. Also, data-sharing with the United States has presented a challenge in Hong Kong. Unlike other SFI locations, there is no law in Hong Kong that permits Hong Kong Customs and Excise (HKCE) to share export data with the U.S. Government. As a result, the United States receives the information directly from MTL. Another unique aspect to Hong Kong is that the equipment is largely vendor-owned, and equipment procurement by the United States was limited. DOE did, however, provide hand-held radiation detection and radioisotope identification equipment and Central Alarm Station (CAS) equipment to Hong Kong. Nevertheless, the equipment experiences downtime similar to other locations. A third issue of note in Hong Kong is that, due to health and safety concerns, all truckers entering the port have a choice of whether or not to drive through the SFI systems.

Busan, Korea

SFI in Port Busan is in operational testing and has already yielded lessons and benefited from SFI experiences in other ports such as Southampton, Honduras, and Qasim. The government of Korea, as well as the terminal operator, Hutchison Port Holdings (HPH), have been strong partners and supporters of the pilot and have facilitated many of remedies to challenges that arise.

Some of the chief challenges in Busan include union health and safety concerns with truckers using the NII equipment, the SAIC P-7500. While the government of Korea is satisfied with the independent reviews outlining the safety of the P-7500, and officials have personally studied the machine, the Korean trucker's union still expresses concerns. Other complications included export licensing for the P-7500 and staffing concerns for the pilot. However, all challenges have been remedied, and operational testing began in late May 2008.

Singapore

The SFI DOP was signed by the U.S. Ambassador to Singapore and the Permanent Secretary of the Ministry of Transport (MOT) for the Republic of Singapore on December 17, 2007. However, negotiations on the details of the Singapore installation have not been finalized. The most important detail to be resolved is whether or not

Singapore would require CBP and DOE to remove the equipment provided after a period of six months. Singapore advised CBP and DOE of this requirement in the fall of 2006, and this has required CBP and DOE to consider changes in the overall design as well as the equipment to be deployed. Consequently, the timelines for delivery of equipment and construction are not fully clear and the operational start date has also been affected. CBP and DOE are in the process of adjusting to Singapore's requirements.

Discussions also continue on various other subjects including: CONOPS, cost reimbursement, staffing, Singapore's post-pilot commitment to the project and who will bear various liabilities. This adds time to construction schedules and delays operational start dates.

Although operations have been delayed, Singapore remains an important partner. The government's historical support of DHS/DOE initiatives such as CSI, C-TPAT, and the Megaports Initiative demonstrate its commitment to collaborating on supply chain security.

Port of Salalah, Oman

The seaport at Salalah, Oman, was designated an SFI port in December 2006, after becoming both a CSI and Megaports port in November 2005. The initial negotiations, started under Megaports and continuing under SFI, have been completed and development of operational deployment timelines is ongoing. Both processes have yielded valuable lessons. Chief challenges include adequate IT infrastructure to transport data to CBP targeters; sufficient staffing levels of both CBP and Omani officials; and designing a CONOPS that works with the limited space available at the port. The Oman government and Port of Salalah have been very cooperative and valuable partners in determining solutions that will ensure the success of the project and prevent detrimental effects on port operations.

Discussion

An evaluation of the need and feasibility of expanding the integrated scanning system to other CSI ports

Continuing operations in some of the current SFI pilot port locations will afford CBP the opportunity to explore possible solutions to the complex challenges posed by transshipment and high-volumes of cargo. However, future deployments will focus on high-risk trade corridors. This strategy will explore efficient expansion options that minimize costs and disruptions to port operations abroad and to the global supply chain in general, while confining deployments to trade lanes that present the greatest risk. This responsible prioritization of departmental resources will ensure that CBP can best enhance security and realize the benefits of the scan data in an efficient manner that does not adversely impact global trade and that recognizes the need to utilize limited resources to address other important vulnerabilities.

The collaborative efforts between DHS and DOE to deploy integrated scanning equipment to the three initial SFI pilot ports in Honduras, the United Kingdom, and Pakistan have demonstrated the feasibility of capturing additional data points (including a radiation scan and image) on U.S.-bound maritime containers on a limited scale, and in locations where a variety of supportive factors exist. This framework of supportive, which cannot be expected to exist in the more than 700 ports shipping to the United States, includes host nation cooperation, low transshipment rates, relatively low volumes of cargo, and technology and infrastructure costs covered primarily by the United States. The successes achieved in these pilot locations, while laudable, were on a narrow scale and have been largely eclipsed by the variety of considerable challenges that arose. As DHS and DOE worked under tight deadlines to meet SAFE Port Act international scanning pilot port requirements, many challenges were addressed on a case-by-case basis with a variety of innovative operational solutions, necessary compromises, and temporary agreements. The conclusion to draw from the experiences with these initial SFI ports is that they are not representative of, or templates for, complete scanning operations at other international locations.

The pilots have also demonstrated that the additional data elements, if incorporated into the risk-based methodology and used to augment the information CBP already receives under the 24-Hour Rule and will soon receive under the Advanced Security Filing, have the potential to enhance targeting efforts in specific situations. While the data can be useful, the expenses are substantial and key challenges will need to be addressed as the U.S. Government considers additional deployments.

Some of the most significant challenges are the difficulties associated with capturing scan data on transshipped cargo and identifying protocols, policies and port infrastructure modifications that will permit scanning at high volume locations without impacting the movement of goods through the port and through the global supply chain. The initial SFI/ICS deployments have demonstrated the technical feasibility of integrating the various components of the scanning process, as well as the more operational feasibility of capturing this data in low-volume ports that process mostly gate traffic. However, as negotiations in the high volume and high transshipment ports of Singapore and Salalah demonstrated, developing and executing realistic concepts of operation in these more challenging environments is difficult.

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

As DHS develops a policy for future expansion, in conjunction with DOE and DOS, we must acknowledge both the diplomatic and operational challenges encountered in the first phase of deployments. Based on preliminary results from the three pilot locations, and in light of the considerable costs and challenges associated with the deployment of SFI/ICS systems, we will focus departmental resources on scanning in specific high risk trade corridors, where the most security benefit can be realized. This approach accords with our risk-based strategy, best addresses the greatest potential threats to the United States, and represents the most worthwhile investment of limited available resources for the scanning of cargo containers at foreign ports.

Conclusion

A critical element of any strategy to protect our nation is monitoring what is coming across our borders. Physically inspecting every single container that enters the country would be impractical and detrimental to our own economy, as well as the global economy, and extreme. Instead, we rely on a robust layered, risk-management approach that identifies and focuses our resources on threats while allowing legitimate cargo to move unhindered through the process. This risk-based and approach reduces the likelihood of a successful exploitation of any one layer in the supply chain system as a whole. The appropriate distribution of limited resources, based on informed judgment regarding the totality of dangers facing the nation, is a necessary precondition to the success of this risk-based and layered approach. The evolving nature of threats against the United States, and the attractiveness of exploiting any point of least resistance, is a call for vigilance against a disproportionate expenditure of resources and attention in one area, to the potential detriment of other vital less fortified vulnerabilities.

Significant lessons have been learned from the initial SFI pilot ports established over the last year, in close partnership with DOE. The initial three ports demonstrated that the scanning of all U.S-bound maritime containers is possible on a limited scale. These ports benefited from having host nation cooperation, low cargo volumes, low transshipment rates, and technology and infrastructure costs covered primarily by the United States Government, where available. These supportive conditions do not exist in all ports shipping to the United States, so DHS must prioritize deployments in a manner that maximizes the security benefit, minimizes disruptions to port operations and the global supply chain, and maintains cost efficiency.

The costs associated with the establishment of a SFI/ICS port and with the equipment and personnel necessary to collect, analyze, and transfer scan data obtained through SFI integrated systems are reasonable and necessary expenditures to the degree that increased security results. An approach that prioritizes deployments to high-risk trade corridors and continues operations in some of the initial pilot ports will provide CBP the opportunity to expend resources and efforts on the development of the technology and operational solutions necessary to address key challenges (such as transshipment), while obtaining additional information on cargo traveling through trade corridors that warrant additional scrutiny. Capturing scan data on transshipments without seriously impacting port operations is rendered all the more difficult by the characteristics of this type of cargo: shorter dwell times, space constraints, availability of shipping data, and the difficulty of identifying chokepoints within the container terminals. Advancements in transshipment technologies, including mobile and spreader bar technologies (should they prove to be technically viable) will help address challenges posed by heavy transshipment ports.

Sustained operations in some of the initial SFI/ICS locations, in combination with deployments to additional ports, will provide continuing opportunities to develop solutions to some of the more challenging hurdles encountered thus far. As DHS, working closely with DOE and DOS, expands international scanning responsibly and

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

efficiently, the focus will be on high-risk trade corridors that represent the greatest threat to the United States. This corridor approach will direct limited departmental resources toward those areas where the most benefit can be derived from the incorporation of the additional scan data into CBP's targeting systems and, more broadly, into CBP's effective risk-based strategy. Such a strategy is also consistent with the risk-based approach DOE employs in its Megaports Initiative. CBP will continue coordinate with DOE on future SFI expansion.

Central to the SFI program and to DHS's mission in general, is the conviction that reliable information obtained earlier in the shipping process supports and enhances the ability of CBP Officers to distinguish between legitimate commerce and potential threats. The integrated scanning systems have proven capable of producing, collecting, and transmitting scan data points. These additional data enhance the targeting process by providing CBP with helpful insight regarding the security of a container's contents as it transits to the United States. As technology matures, additional benefits may be derived from automatic anomaly detection capabilities that would ease the burden on the highly trained personnel now required to review and analyze scan data. An expansion approach that focuses on high-risk trade corridors will allow CBP to maximize the benefit that can be derived from the additional information.

While the scan data can be useful, the costs associated with obtaining it, even in the limited number of current SFI pilot ports, have proven significant. DHS and DOE funded the initial phase of SFI deployments, committing a combined total of approximately \$60 million to the program. The resources committed by DHS and DOE greatly minimized the costs to the terminal operators and industry and foreign partners. Nevertheless, our partners in this effort incurred considerable costs, including expenditures related to staffing increases, local information technology and terminal operating system enhancements, fuel, and other program support functions. USG expenditures during the 6 month pilot phase addressed the material costs associated with equipment, personnel, facilities, and information and communication enhancements. More intangible costs associated with potential increases in wait times at higher-volume ports, more extensive infrastructure modifications that will be necessary to address transshipments and non-gate traffic, and the impact of these additional requirements on the speed and efficiency of trade flow both through specific port operations and to the United States, remain unknown. The extensive costs and operational, technical and diplomatic hurdles of expanding the SFI/ICS program to the more than 700 ports that ship to the United States necessitates a path forward that will incorporate scan data as an additional layer in the robust risk-management approach we have in place and will focus future scanning deployments on high-risk trade corridors.

Acronyms

ASP – Advanced Spectroscopic Portal

ATS – Automated Targeting System

CAS – Central Alarm System

CBP – U.S. Customs and Border Protection

CBR – Central Board of Revenue

CERTS – Cargo Enforcement Reporting and Tracking System

CITOS – Computer Integrated Terminal Operating System (Singapore)

CONOPS – Concept of Operations

CSI – Container Security Initiative

CSDRD – Communications System Design Requirements Document

C-TPAT – Customs – Trade Partnership Against Terrorism

DEI – Direccion Ejecutiva de Ingressos (Honduran Customs)

DHS – Department of Homeland Security

DNDO – Domestic Nuclear Detection Office

DOC – U.S. Department of Commerce

DOD – U.S. Department of Defense

DOE – U.S. Department of Energy

DOP – Declaration of Principles

DOS – U.S. Department of State

DPW – Dubai Ports World

FSN – Foreign Service National

FY – Fiscal Year

HKCE – Hong Kong Customs and Excise

HMRC – Her Majesty's Revenue and Customs (U.K.)

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

HPH – Hutchison Port Holdings

HSC – Health and Safety Commission (U.K.)

IC3 – Integrated Cargo Container Control

ICA –Immigrants and Checkpoints Authority (Singapore)

ICE – Immigration and Customs Enforcement

ICIS – Integrated Container Inspection System

ICS – International Container Security

IRR – Ionizing Radiation Regulations (U.K.)

IT – Information Technology

IP – Internet Protocol

KCS – Korea Customs Service

KINS – Korean Institute of Nuclear Safety

LPR – License Plate Reader

LSS – Laboratories and Scientific Services

MI – Megaports Initiative

MOT – Ministry of Transport (Singapore)

MOU – Memorandum of Understanding

MPA – Maritime and Port Authority of Singapore

MTL – Modern Terminal LTD (Hong Kong)

NDC – National Data Center

NEEMR – National Enforcement Equipment Maintenance and Repair

NII – Non-intrusive Inspection

NNSA – National Nuclear Security Administration

NORM – Naturally Occurring Radioactive Material

NTC-C – National Targeting Center - Cargo

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

OCR – Optical Character Recognition

OIT – Office of Information and Technology

PNNL – Pacific Northwest National Laboratory

PSA – Port of Singapore Authority

RFP – Request for Proposal

RIID – Radiation Isotope Identification Device

ROP – Royal Omani Police

RPA – Radiation Protection Advisor (U.K.)

RPM – Radiation Portal Monitor

RSO – Radiation Safety Officer

SAIC – Science Applications International Corporation

SCT – Southampton Container Terminals

SERNA – Secretaria de Recursos Naturales y Ambiente

SFI – Secure Freight Initiative

SLD – Second Line of Defense

SNM – Special Nuclear Material

SPOG – SFI Project Operations Group (Singapore)

TDY – Temporary Duty

TCP – Transmission Control Protocol

TOS – Terminal Operating System

U.K. – United Kingdom

UAE – United Arab Emirates

UKAEA – United Kingdom Atomic Energy Authority

UPS – Uninterruptible Power Supply

U.S. – United States

REPORT TO CONGRESS ON INTEGRATED SCANNING SYSTEM

FOR PUBLIC RELEASE

VACIS – Vehicle and Cargo Inspection System (SAIC imaging device)

VAT – Value Added Tax

^3He – Helium 3

^{239}Pu –Plutonium- 239

^{235}U –Uranium- 235

^{241}Am – Americum 241