



# governmentattic.org

*"Rummaging in the government's attic"*

Description of document: Customs and Border Protection (CPB) Unpublished Reports to Congress, 2009-2010

Appeal date: 17-August-2010

Released date: 30-September-2010

Posted date: 27-May-2013

Source of document: US Customs and Border Protection  
FOIA Division  
799 9th Street NW, Mint Annex  
Washington, DC 20229-1181  
Email: [CBPFOIA@DHS.gov](mailto:CBPFOIA@DHS.gov)  
Fax: (202) 325-023

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



**U.S. Customs and  
Border Protection**

OT: RR: FAPL  
H120615MBP

SEP 30 2010

RE: Freedom of Information Act Appeal; File No. 2010F15489

This letter responds to your appeal of the production you received from Dorothy Pullo, Director, FOIA Division, in response to your Freedom of Information Act ("FOIA") request. On July 1, 2010, The Department of Homeland Security (DHS) referred 42 pages that it had identified as belonging to Customs and Border Protection (CBP) when responding to your February 14, 2010 FOIA request. On August 11, 2010, Ms. Pullo provided you with seven of those pages, with some redactions, and withheld another 35 pages of records, in full, pursuant to exemptions located with the FOIA.

On August 17, 2010, you appealed those redactions, contending that CBP failed to perform its statutory duty under the FOIA to release all segregable, non-exempt portions of the records at issue and ignored President Obama's and Attorney General Holder's memoranda on the FOIA instructing agencies on the presumption of openness the Act. We agree and grant your appeal, releasing the additional records and information attached to this letter.

**Release of Additional Records**

The Freedom of Information Act was enacted to "ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." *Nat'l Labor Relations Bd. v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978). The law provides the public with the right to receive records and information from the government in order to further democratic principles and allow for independent evaluation of government action.

As you noted in your appeal letter, President Barack Obama, in his first day in office, issued a memorandum that made clear that his administration would dedicate itself to the principles that motivated Congress to enact the FOIA. The President explained that "accountability requires transparency" and demanded that federal agencies "adopt a presumption in favor of disclosure in order to renew their commitment to the principles embodied in FOIA, and to usher in a new era of open Government."

In furtherance of those interests, both I and another attorney in my office re-reviewed the information withheld from the original production. As a result of this examination, we have released, with some redactions, all 35 previously withheld pages of records as well as some of the information withheld in Ms. Pullo's initial release. You can find these pages attached to this letter.

Some of the information found in the provided documents has remained redacted. Although the Supreme Court has read the FOIA to espouse "a general philosophy of full agency disclosure," some governmental information is exempted under clearly delineated statutory language. *Dep't of the Air Force v. Rose*, 425 U.S. 352, 360-61 (1976). Thus, while "disclosure, not secrecy, is the dominant objective of [FOIA]," there are some records that exist outside the statute's broad reach. *Id.* Several of those exemptions outlined in the Act – specifically, those described in sections (b)(2), (b)(5), (b)(6), (b)(7)(C), and (b)(7)(E) – apply to information found in the documents produced here.

We have provided you with the greatest amount of information possible. The direct language of the Freedom on Information Act instructs federal agencies to provide any "reasonably segregable portion of a record" to "any person requesting such record after deletion of the portions which are exempt." §552(b). To comport with this requirement, this office "differentiate[d] among the contents of a document rather than to treat it as an indivisible 'record' for FOIA purposes." *Fed. Bureau of Investigation v. Abramson*, 456 U.S. 615, 626 (1982). Only the information protected by the statutorily defined exemptions has been blacked out on your copies of the records.

### **Application of Exemption (b)(2)**

Exemption (b)(2) of the FOIA exempts from mandatory disclosure records that are "related solely to the internal personnel rules and practices of an agency." 5 U.S.C. § 552(b)(2). Courts interpret Exemption (b)(2) to encompass two distinct categories of information, the first of which – referred to as "low 2" information - covers predominantly internal documents that deal with "trivial administrative matters of no genuine public interest." *Schiller v. Nat'l Labor Relations Bd.*, 964 F.2d 1205, 1207 (D.C. Cir. 1991) (internal quotation marks omitted). In accordance with Attorney General Eric Holder's March 19, 2009 FOIA memorandum instructing that government agencies "not withhold records merely because it can demonstrate, as a technical matter, that the records fall within the scope of a FOIA exemption," and despite your concern that "CBP routinely cited low b(2) in its determinations," we have released all "low 2" information found within these records.

The second subset of information protected by Exemption b(2) – referred to as "high 2" information - applies to "[p]redominantly internal documents the disclosure of which would risk circumvention of agency statutes and regulations." *Schiller*, 964 F.2d at 1207. Information excluded from disclosure under the "high 2" exemption must withstand a two-step examination. *Elliott v. USDA*, 2010 U.S. App. LEXIS 4031 (D.C. Cir. Feb. 26, 2010). As an initial matter, the material must fall within the language of the statute. That is, it must be "used for predominantly internal purposes," and relate to "rules and practices for agency personnel." *Crooker v. Bureau of Alcohol, Tobacco & Firearms*, 670 F.2d 1051, 1073 (D.C. Cir. 1981).

Once this initial threshold is overcome, the public interest in obtaining the material is legally irrelevant. See *Voinche v. Fed. Bureau of Investigation*, 940 F. Supp. 323, 328 (D.D.C. 1996). Instead, the sole consideration in determining whether information is properly exempted is where disclosure “significantly risk[s] circumvention of federal regulations or statutes.” *Crooker* 670 F.2d at 1074. This is because the concern in such cases is that a FOIA disclosure should not “benefit those attempting to violate the law and avoid detection.” *Id.* at 1053.

Here, Exemption (b)(2) has been used to redact information related to the rules and practices of CBP’s scanning program for all U.S.-bound maritime shipments. Although you yourself may not seek this information for nefarious purposes, “it would appear obvious that those immediately and practically concerned with such matters would be individuals embarked upon clandestine and illicit operations, the detection of which would be frustrated if they were privy to the methods employed... to ferret them out.” *Caplan v. Bureau of Alcohol, Tobacco & Firearms*, 587 F.2d 544, 547 (2d Cir. 1978); see also *Buffalo Evening News, Inc. v. U.S. Border Patrol*, 791 F. Supp. 386, 393 (W.D.N.Y. 1992) (protecting records that “would clearly disclose the USBP’s techniques for apprehending excludable aliens”). As such, these practices have been properly redacted under Exemption (b)(2) from the attached records.

#### **Application of Exemption (b)(5)**

Exemption (b)(5) was designed to “protect the quality of agency decision-making by preventing the disclosure requirement of the FOIA from cutting off the flow of information to agency decisionmakers,” *Mead Data Cent., Inc. v. United States Dep’t of the Air Force*, 566 F.2d 242, 252 (D.C. Cir. 1977), and covers “inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency.” § 552(b)(5). It exempts “those documents, and only those documents, normally privileged in the civil discovery context.” *Nat’l Labor Relations Bd. v. Sears Roebuck & Co.*, 421 U.S. 132, 149 (1975).

The rationale behind the deliberative process privilege – one of three protected by the exemption – is that public disclosure of deliberative, predecisional documents would prevent “the full and frank exchange of ideas” from “flowing freely” within government agencies. *Mead Data Cent.*, 566 F.2d at 256. Indeed, in applying the privilege in an analogous context, the Supreme Court recognized that “[h]uman experience teaches that those who expect public dissemination of their remarks may well temper candor with a concern for appearances... to the detriment of the decisionmaking process.” *United States v. Nixon*, 418 U.S. 683, 705 (1974).

The privilege therefore “serves to assure agency employees that they can provide a decisionmaker with their uninhibited opinion without fear of public scrutiny, to prevent premature disclosure of proposed policies, and to protect against public confusion through the disclosure of document advocating or discussing reasons for policy decisions that were ultimately not adopted.” *Kidd v. Dep’t of Justice*, 362 F. Supp. 2d 291, 296 (D.D.C. 2005). As is the case here, because the exemption protects the deliberative process and not necessarily the substance of the records, it continues to apply even after the agency has made

a final determination on the subject matter the records address. *Elec. Privacy Info. Ctr. v. Dep't of Homeland Sec.*, 384 F. Supp. 2d 100, 112-113 (D.D.C. 2005) (“Contrary to plaintiff’s assertion that materials lose their Exemption 5 protection once a final decision is taken, it is the document’s role in the agency’s decision-making process that controls”).

To invoke the privilege, the records must be both predecisional and deliberative. *Wolfe v. Dep't of Health & Human Servs.*, 839 F.2d 768, 774 (D.C. Cir. 1988). A predecisional record is one that is “antecedent to the adoption of an agency policy.” *Elec. Privacy Info. Ctr.*, 384 F. Supp. 2d at 112. That is, it must be generated as part of a continuing process of agency decision-making. *Nat'l Ass'n of Home Builders v. Norton*, 309 F.3d 26, 39 (D.C. Cir. 2002) (holding that a document is predecisional if it was prepared to assist an agency in arriving at a decision, rather than supporting a decision already made). A deliberative process is one that plays “a direct part of the deliberative-process in that it makes recommendations or express opinions on legal or policy matters.” *Public Citizen, Inc. v. Office of Mgmt. and Budget*, 598 F.3d 865, 876 (D.C. Cir. 2009). The “key question” in identifying “deliberative” material is whether disclosure of the information would “discourage candid discussion within the agency.” *Access Reports v. Dep't of Justice*, 926 F.2d 1192, 1195 (D.C. Cir. 1991).

In the instant case, Exemption (b)(5) is being used largely to protect information in a report to Congress prepared by CBP on the Integrated System Scanning Pilot. It has also been applied to a very small amount of information found in a report on the Secure Border Initiative. The redacted sections of the reports provide the opinions, analysis and interpretations of CBP employees related to the implementation of an integrated scanning system aimed at examining 100 percent of U.S.-bound maritime containers and the impact of tactical infrastructure on border security.

These recommendations and opinions are of the exact type of records contemplated by Congress in enacting Exemption (b)(5). *Sears*, 421 U.S. at 150 (noting that the “focus” of the Exemption is on records “reflecting advisory opinions, recommendations and deliberations comprising part of a process by which governmental decisions and policies are formulated”). The release of these internal documents would “stifle honest and frank communication within” CBP, and potentially prevent the free flow of information from reaching key decisionmakers within the agency. *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 866 (D.C. Cir. 1980). Doing so would inevitably result in diminished work product and uneven or inappropriate application of customs laws.

#### **Application of Exemptions (b)(6) and (b)(7)(C)**

Exemptions (b)(6) and (b)(7)(C) both relate to protecting personal privacy and have been invoked here to protect the signature of Chani Wiggins, Assistant Secretary of the Office of Legislative Affairs. Under the Freedom of Information Act, privacy encompasses the “individual’s control of information concerning his or her person.” *Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989). Exemption 6 protects “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.” § 552(b)(6). Exemption (b)(7)(C) excludes records or information compiled for law enforcement purposes, but only to the extent that the

production of such materials “could reasonably be expected to constitute an unwarranted invasion of personal privacy.” § 552(b)(7)(C). To determine whether this information ought to be upheld under either exemption, an agency must balance the privacy interests involved against the public interest in disclosure. *Reporters Comm. for Freedom of the Press*, 489 U.S. at 762.

As a threshold requirement, Exemption (b)(6) can only be applied to “personnel and medical and similar files.” 5 U.S.C. § 552(b)(6). However, the range of documents falling within these categories is interpreted broadly so as to include all government records “which can be identified as applying to that individual.” *Dep’t of State v. Washington Post*, 456 U.S. 595, 602 (1982) (quoting H. R. Rep. No. 1497, 89th Cong., 2nd Sess., 11 (1966)). Once this threshold is met, the issue becomes whether disclosure of the information at issue “would constitute a clearly unwarranted invasion of personal privacy,” *Rose*, 425 U.S. at 373, an undertaking that requires balancing the privacy interests of the individual against the public interest in disclosure. That balance can be properly struck where “personal references or other identifying information [are] deleted.” *Id.* at 380.

In order to compel release of materials, there must be at least some public interest in their disclosure because “something, even a modest privacy interest outweighs nothing every time.” *Cappabianca*, 847 F. Supp. at 1564. In this case, you do not argue what benefits to the public might stem from releasing Ms. Wiggins’ signature. However, it seems that its release, on its own, is unlikely to further the goals of the FOIA, namely “to open agency action to the light of public scrutiny.” *Rose*, 425 U.S. at 372. Without any genuine, public interest, there is little reason to identify the third parties found in these documents. Accordingly, Exemption (b)(6) has been applied here to withhold Ms. Wiggins’ signature.

Although the protections available under Exemption (b)(7)(C) are not the same as Exemption (b)(6), the analysis is the same, requiring the balance of the privacy interests involved against the public interest in disclosure. *Lewis v. Dep’t of Justice*, 609 F.Supp.2d 80, 84 (D.D.C. 2009). However, because exemption (b)(7)(C) contains broader protections than exemption b(6)<sup>1</sup>, the two exemptions differ in the “magnitude of the public interest that is required” to overcome the privacy interests involved, with an extra thumb on scale in favor of redaction once Exemption b(7)(C) privacy issues are implicated. *Dep’t of Defense v. Fed. Labor Relations Auth.*, 510 U.S. 487, 496 n.6 (1994).

Like Exemption (b)(6), Exemption (b)(7)(C) has also been found to protect the privacy interests of all persons mentioned in law enforcement records, including investigators, suspects, witnesses and informants. *Lewis*, 609 F. Supp. 2d at 84. The privacy interest at play under Exemption (b)(7)(C) in protecting the third party information located in law enforcement documents is so strong, though, that courts have found that such information is

---

<sup>1</sup> Exemption (b)(7)(C)'s privacy language is broader than the comparable language in exemption 6 in two respects. First, whereas Exemption 6 requires that the invasion of privacy be “clearly unwarranted,” the adverb “clearly” is omitted from Exemption 7(C). Second, whereas Exemption 6 refers to disclosures that “would constitute” an invasion of privacy, Exemption 7(C) encompasses any disclosure that “could reasonably be expected to constitute” such an invasion. *Dep’t of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. at 762

“categorically exempt” from production “unless access to the names and addresses of private individuals... is necessary in order to confirm or refute compelling evidence that the agency is engaged in illegal activity.” *SafeCard Services, Inc. v. U.S. Sec. & Exchange Comm’n.*, 926 F.2d 1197, 1206 (D.C. Cir. 1991).

Once the threshold requirement that the information be found in “law enforcement” records is met<sup>2</sup> and the privacy interests described in Exemption (b)(7)(C) are triggered, the onus shifts to the requester to show government misconduct. *Nat’l Archives & Records Admin. v. Favish*, 541 U.S. 157, 172 (2004). That showing must be “more than a bare suspicion” of official misconduct – it must “warrant a belief by a reasonable person that the alleged Government impropriety might have occurred.” *Id.* at 174. Otherwise, the balancing requirement does not come into play. *Boyd v. Dep’t of Justice*, 475 F.3d 381, 388 (D.C. Cir. 2007). Having determined the information found in question to be located in a law enforcement record and without any evidence indicating misconduct, Ms. Wiggins’ signature has been redacted.

### **Application of Exemption (b)(7)(E)**

Exemption (b)(7)(E) exempts material that was compiled for law enforcement purposes and that would disclose the “techniques and procedures” or “guidelines” for “law enforcement investigations or prosecutions.” Application of this exemption is limited, however, to cases in which disclosure “could reasonably be expected to risk circumvention of the law.” 5 U.S.C. § 552(b)(7)(E). Like Exemption b(7)(C), information that falls within Exemption b(7)(E)’s purview is “categorically exempt” from disclosure. *Fisher v. Dep’t of Justice*, 772 F.Supp. 7, 12 at n. 9 (D.D.C. 1991).

In this case, the information redacted in accordance to Exemption b(7)(E) describes strengths and weakness of certain law enforcement resources, challenges associated with certain law enforcement techniques, law enforcement techniques related to monitoring the scanning process, location of certain law enforcement resources, specialized law enforcement procedures utilized at specific locations, strengths and weakness of certain law enforcement techniques, information about law enforcement techniques that would reveal weaknesses, photographs and detailed diagrams of the lay out scanning systems, targeting procedures utilized by special teams, and detailed information regarding the software used in scanning containers.

Disclosure of this information would compromise both CBP’s as well as other federal agencies’ ability to enforce and prosecute persons for violations of these laws. Releasing this information could reveal a great deal of information related to the law enforcement techniques used to scan and evaluate maritime containers entering the United States and has therefore been properly redacted. See *Pons v. U.S. Customs Serv.*, 1998 U.S. Dist. LEXIS 6084 (D.D.C. Apr. 23, 1998) (upholding use of Exemption b(7)(E) to protect descriptions of law

---

<sup>2</sup> It is well established that CBP has a law enforcement mandate. *Coastal Delivery Corp. v. U.S. Customs Serv.*, 272 F. Supp. 2d 958, 963 (C.D. Cal. 2003). The records in this case were compiled for the purpose of scanning and evaluating shipments of goods into the United States and securing this nation’s borders. They are in clear furtherance of that law enforcement mandate.

enforcement techniques and the secrecy of cooperative efforts). Doing so could enable circumvention of the examination procedures developed by CBP, and these records are properly withheld.

In the event that you are dissatisfied with the disposition of your appeal, you may obtain judicial review of this decision pursuant to the provisions of 5 U.S.C. §552(a)(4)(B) in the United States District Court in the District in which you reside, in the District where the agency records are situated, or in the United States District Court for the District of Columbia.

Sincerely,

A handwritten signature in black ink, appearing to read "Shari Suzuki". The signature is fluid and cursive, with the first name "Shari" being more prominent than the last name "Suzuki".

Shari Suzuki, Chief  
FOIA Appeals, Policy and Litigation Branch

JAN 04 2010

Assistant Secretary for Legislative Affairs  
U.S. Department of Homeland Security  
Washington, DC 20528



# Homeland Security

Pursuant to the requirements of 31 U.S.C. Section 720, the Department of Homeland Security (DHS) is submitting this written statement on actions taken regarding the Government Accountability Office (GAO) recommendations contained in its report, GAO-09-873, *Food Safety: Agencies Need to Address Gaps in Enforcement and Collaboration to Enhance Safety of Imported Food*.

This letter provides a status update on efforts to implement the GAO recommendations contained in the report and is being provided to the following Members of Congress and the Director of OMB:

The Honorable Bennie G. Thompson  
Chairman, Committee on Homeland Security

The Honorable Peter King  
Ranking Member, Committee on Homeland Security

The Honorable Edolphus Towns  
Chairman, Committee on Oversight and Government Reform

The Honorable Darrell Issa  
Ranking Member, Committee on Oversight and Government Reform

The Honorable Joseph I. Lieberman  
Chairman, Committee on Homeland Security and Governmental Affairs

The Honorable Susan M. Collins  
Committee on Homeland Security and Governmental Affairs

The Honorable Peter Orszag, Director  
Office of Management and Budget

I appreciate your interest in the Department of Homeland Security. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 447-5890.

Respectfully,

(b)(6), (b)(7)(C)

  
Chani Wiggins  
Assistant Secretary  
Office of Legislative Affairs

Pursuant to the requirements of 31 U.S.C. Section 720, the Department of Homeland Security (DHS) is submitting this written statement on actions taken regarding the Government Accountability Office (GAO) recommendations contained in its report, GAO-09-873, *Food Safety: Agencies Need to Address Gaps in Enforcement and Collaboration to Enhance Safety of Imported Food*.

**Recommendation #1**

To ensure that Food and Drug Administration (FDA) and Food Safety and Inspection Service (FSIS) receive the information they need to adequately oversee imported food safety, we recommend that the CBP Commissioner ensure that CBP's new screening system communicates time-of-arrival information to the FDA and FSIS screening systems.

**Update**

Once CBP begins gathering time-of-arrival data in its new screening system, CBP will have the capability to provide that data to FDA and FSIS provided that FDA and FSIS requests, and have the legal authority to collect, the information.

**Recommendation # 2:**

Until this new system is capable of communicating this information, we recommend that CBP implement its interagency agreement with FDA to provide time-of-arrival information and explore opportunities to implement a similar agreement with FSIS.

**Update**

The CBP Office of Information and Technology (OIT), has a plan that includes actions to implement the interagency agreement with FDA mentioned above and correspondence with Office of International Trade (OT) towards implementing a similar agreement with FSIS. This action is dependent on a request from FSIS. OIT completed the development of the modification to the software that will provide the FDA with the transmission of the conveyance/information arrival message for truck and air shipments. Currently, OIT is testing the modification between OIT and FDA systems. Based on the results, the modification is planned to be delivered to FDA on March 2010.

**Recommendation # 5:**

To improve CBP's and FDA's ability to identify foreign firms with violative histories, we recommend the CBP Commissioner should ensure that ACE is able to accept a unique identification number for foreign firms that export FDA-regulated foods.

**Update**

CBP OIT has developed a plan that includes a specification that ACE shall accept a unique identification number for foreign firms that export FDA regulated foods or other entities so designated by a Participating Government Agency (PGA). At present it is planned that CBP's Office of Trade will develop and distribute the CBP International Trade Data System Concept of Operations (CONOPS) which will determine CBP's decisions on the cargo release process in ACE. The CONOPS is to be delivered on February 2010.

**Recommendation #7**

To enhance agency coordination and to streamline FDA's refusal process with CBP's redelivery process, we recommend that the FDA Commissioner and the CBP Commissioner jointly study, with input from agency field officials, ports where a joint initiative would be feasible.

**Update**

CBP and FDA have begun discussions on a joint form as a prerequisite to considering this joint notice as a national procedure. Additional discussions are needed to complete this evaluation, after which we hope that national procedures can be drafted, cleared, and implemented.

NOV 02 2009



**Homeland  
Security**

Pursuant to the requirements of 31 U.S.C. Section 720, the Department of Homeland Security (DHS) is submitting this written statement on actions taken regarding the Government Accountability Office (GAO) recommendations contained in its report, GAO-09-896, **SECURE BORDER INITIATIVE: Technology Deployment Delays Persist and the Impact of Border Fencing Has Not Been Assessed.**

This letter is being provided to the following Members of Congress and the Director of OMB:

**The Honorable Bennie G. Thompson**  
Chairman, Committee on Homeland Security

**The Honorable Peter King**  
Ranking Member, Committee on Homeland Security

**The Honorable Edolphus Towns**  
Chairman, Committee on Oversight and Government Reform

**The Honorable Darrell Issa**  
Ranking Member, Committee on Oversight and Government Reform

**The Honorable Joseph I. Lieberman**  
Chairman, Committee on Homeland Security and Governmental Affairs

**The Honorable Susan M. Collins**  
Ranking Member, Committee on Homeland Security and Governmental Affairs

**The Honorable Peter Orszag, Director**  
Office of Management and Budget

I appreciate your interest in the Department of Homeland Security. If I may be of further assistance, please contact me at (202) 447-5890.

Sincerely,

(b)(6) (b)(7)(C)

**Chan Wiggins**  
Assistant Secretary  
Office of Legislative Affairs

Pursuant to the requirements of 31 U.S.C. Section 720, the Department of Homeland Security (DHS) is submitting this written statement on actions taken regarding the Government Accountability Office (GAO) recommendations contained in its report, GAO-09-896, SECURE BORDER INITIATIVE: Technology Deployment Delays Persist and the Impact of Border Fencing Has Not Been Assessed.

The report contained one recommendation. U.S. Customs and Border Protection (CBP) concurred with the recommendation. The recommendation and CBP's updated actions to address the recommendation are described below.

**Recommendation:** "To improve the quality of information available to allocate resources and determine tactical infrastructure's contribution to effective control of the border, we recommend that the Commissioner of CBP conduct a cost-effective evaluation of the impact of tactical infrastructure on effective control of the border."

**CBP Update:** In our effort to improve our ability to effectively measure the impact of tactical infrastructure on the border, officials from CBP's Office of Border Patrol (OBP) met with a representative from the University of Arizona on September 24, 2009, to discuss the need to analyze the impact of tactical infrastructure on border security. The University of Arizona<sup>(b) (5)</sup>

(b) (5)

(b) (5) However, prior to taking advantage of this DHS relationship, OBP had to first review current contracts to ensure that there was no duplication of effort with other projects. OBP completed this internal review on October 9, 2009. OBP can now begin the process of identifying and selecting the proper contracting vehicle. If funding is available, a contract should be awarded by the end of calendar year 2010. CBP still intends for this comprehensive assessment to be completed no later than the end of calendar year 2011.

NOV 19 2009



## Homeland Security

Pursuant to the requirements of 31 U.S.C. Section 720, the Department of Homeland Security (DHS) is submitting this written statement on actions taken regarding the Government Accountability Office (GAO) recommendations contained in its report, GAO-09-987, *International Trade: U.S. Agencies Have Taken Some Steps, but Serious Impediments Remain to Restricting Trade in Burmese Rubies and Jadeite*.

This letter is being provided to the following Members of Congress and the Director of OMB:

The Honorable Bennie G. Thompson  
Chairman, Committee on Homeland Security

The Honorable Peter King  
Ranking Member, Committee on Homeland Security

The Honorable Edolphus Towns  
Chairman, Committee on Oversight and Government Reform

The Honorable Darrell Issa  
Ranking Member, Committee on Oversight and Government Reform

The Honorable Joseph I. Lieberman  
Chairman, Committee on Homeland Security and Governmental Affairs

The Honorable Susan M. Collins  
Ranking Member, Committee on Homeland Security and Governmental Affairs

The Honorable Peter Orszag  
Director, Office of Management and Budget

I appreciate your interest in the Department of Homeland Security. If I may be of further assistance, please contact me at (202) 447-5890.

Sincerely,

(b)(6) (b)(7)(C)

Chahi Wiggins  
Assistant Secretary  
Office of Legislative Affairs

Pursuant to the requirements of 31 U.S.C. Section 720, the Department of Homeland Security (DHS) is submitting this written statement on actions taken regarding the Government Accountability Office (GAO) recommendations contained in its report, GAO-09-987, International Trade: U.S. Agencies Have Taken Some Steps, but Serious Impediments Remain to Restricting Trade in Burmese Rubies and Jadeite.

“In order to effectively implement the sections of the JADE Act prohibiting the importation of Burmese-origin rubies, jadeite, and related jewelry while allowing imports of non-Burmese-origin goods, we recommend that DHS, in consultation with relevant agencies, develop and implement guidance to conduct postentry reviews of importers’ records and provide improved guidance to importers on the standards of verifiable evidence needed to certify articles are of non-Burmese origin.”

**Recommendation 1:** “To enhance the effectiveness of U.S. policy against the military regime in Burma, we recommend that State, in consultation with DHS and Treasury, analyze the efficacy, challenges, and difficulties faced in implementing measures to restrict trade in Burmese-origin rubies, jadeite, and related jewelry in the context of the broader U.S. sanctions provisions in the JADE Act, and report to Congress how these measures will contribute to its efforts to influence the military regime in Burma.”

**Response/Update:** CBP continues to work alongside the other agencies of the U.S. government to implement the JADE Act within its scope of responsibilities and expertise. Under current direction from the National Security Council, other agencies of the U.S. government are better positioned to identify and are in the process of developing what the U.S. government will rely upon for verifiable evidence for this program. Once such standards are established, CBP will provide improved guidance to importers on the standards of verifiable evidence needed to certify articles are of non-Burmese origin. CBP has begun working on a tasking to conduct post entry reviews of importers’ records to ensure the recordkeeping requirements set out in 19 CFR 12.151(e)(2) are being met.

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE



# Update on Integrated Scanning System Pilot

Fiscal Year 2010 Report to Congress

JANUARY 4, 2010



Homeland  
Security

*U.S. Customs and  
Border Protection*

~~FOR OFFICIAL USE ONLY~~

WARNING: This document is ~~restricted to official use only~~. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOI/O information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

JAN 04 2010

## Foreword

I am pleased to present the following report, "Update on Integrated Scanning System Pilot," which has been prepared by U.S. Customs and Border Protection (CBP).

The report has been compiled in response to a legislative requirement in Section 232(c) of the Security and Accountability for Every Port Act of 2006 (SAFE Port Act), P.L. 109-347. This report is the third of a series of status reports required by Section 232(c), to be provided every six months, on the full-scale deployment of the integrated scanning system to capture 100 percent of U.S.-bound, maritime containers.

The report details status update of container scanning and imaging operations at the Secure Freight Initiative (SFI) locations, as well as advances and enhancements to the SFI software. The report also describes some of the challenges that still exist and reiterates the need to progress with 100 percent scanning in a responsible, deliberate, and risk-based approach.

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

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

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

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

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

The Honorable Bennie G. Thompson  
Chairman, House Committee on Homeland Security

The Honorable Peter T. King  
Ranking Member, House Committee on Homeland Security

The Honorable Joseph I. Lieberman  
Chairman, Senate Committee on Homeland Security and Governmental Affairs

ii

~~FOR OFFICIAL USE ONLY~~

WARNING: This document is ~~classified~~. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

The Honorable Susan M. Collins  
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs

The Honorable James L. Oberstar  
Chairman, House Committee on Transportation and Infrastructure

The Honorable John Mica  
Ranking Member, House Committee on Transportation and Infrastructure

The Honorable Jay Rockefeller  
Chairman, Senate Committee on Commerce, Science, and Transportation

The Honorable Kay Bailey Hutchinson  
Vice Chairman, Senate Committee on Commerce, Science, and Transportation

The Honorable Charles B. Rangel  
Chairman, House Committee on Ways and Means

The Honorable Dave Camp  
Ranking Member, House Committee on Ways and Means

The Honorable Max Baucus  
Chairman, Senate Committee on Finance

The Honorable Charles E. Grassley  
Ranking Member, Senate Committee on Finance

Inquiries relating to this report may be directed to Office of Legislative Affairs at  
(202) 447-5890.

Respectfully,

(b)(6) (b)(7)(C)

  
Chani W. Wiggins  
Assistant Secretary  
Office of Legislative Affairs

iii

~~FOR OFFICIAL USE ONLY~~

WARNING: This document is ~~FOR OFFICIAL USE ONLY~~. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

## Executive Summary

This report is required under Section 232(c) of the SAFE Port Act (6 U.S.C. 982(c)) and describes the status of the full-scale, as well as limited capacity deployments of the integrated scanning systems in foreign ports around the world.

Currently, the Secure Freight Initiative (SFI) deployments are operational in four locations: Southampton, United Kingdom; Qasim, Pakistan; Puerto Cortés, Honduras, and the Gamman Terminal in Busan, South Korea. Additionally, SFI is working to expand deployment operations to the Port of Salalah, Oman and anticipates the full operational testing in October 2009. Additionally, it is important to note that as of April 30, 2009, the SFI pilot study at the Modern Terminal in the Port of Hong Kong officially ended by mutual agreement between the U.S. Department of Homeland Security (DHS) and the Hong Kong Government (HKG). This report provides an update on each port and its equipment, an evaluation of SFI software in use and being developed, and an overview of the strategy that will guide future SFI deployments.

The SFI deployments in the four operational ports continue to yield valuable lessons. As noted in the previous report, the continuation of operations in the current SFI locations affords U.S. Customs and Border Protection (CBP) the opportunity to further test possible solutions to the complex challenges posed by scanning 100 percent of U.S.-bound containers, particularly at transshipment and high-volume ports. However, while the data can be useful, operational costs are significant even in these limited environments. While we continue to learn important lessons in these initial locations, DHS will prioritize future scanning deployments to locations of strategic importance. Focusing deployments in this way will maximize the security and trade facilitation benefits that can be achieved and ensure that CBP has the capacity to compile, assess, and integrate the additional scan data into its effective, functioning risk-based strategy.

As noted in the previous reports, the successful deployment of integrated scanning equipment presents certain diplomatic, technical, and logistical challenges. This report describes the current status of SFI locations; enhancements to SFI software; and some of the ongoing challenges such as obtaining the necessary support of host governments, equipment costs and downtime, operational issues such as port infrastructure constraints, and health and safety concerns regarding the operation of imaging equipment. Furthermore, it reiterates the need to proceed with the SFI program in a responsible, practical manner that best achieves the goal of maximizing the security of U.S.-bound maritime cargo while maintaining an effective risk-based strategy. A prioritized approach that focuses on locations of strategic importance will maximize the security and trade facilitation benefits resulting from the collection of additional scan data; address the requirements of section 1701 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), P.L. 110-53; and ensure the long-term sustainability of the SFI deployments. This approach will also allow DHS to deploy currently available technology

iv

~~FOR OFFICIAL USE ONLY~~

<p>WARNING: This document is <del>unclassified</del>. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.</p>
---

~~FOR OFFICIAL USE ONLY~~  
**LAW ENFORCEMENT SENSITIVE**

while continuing to develop critical improvements to scanning system capabilities, to include automated detection and solutions to the complex challenges associated with transshipped cargo.

DHS continues to encounter several distinct challenges that warrant discussion in this summary. First, maintaining and operating the scanning equipment continues to be a significant challenge to SFI operations. All of the current SFI locations continue to experience scanning equipment and system downtime. The extreme climate conditions, numerous power outages, and disruptions to the communication lines and service have contributed to several instances of equipment and system downtime.

At the Port of Southampton, United Kingdom, several instances of equipment and system downtime continue to be a challenge for SFI scanning operations, although the SFI program has seen improvements since the last report submitted to Congress on March 17, 2009. The Advanced Spectroscopic Portal (ASP) and the imaging system are some of the newest technologies deployed at any port.<sup>1</sup> These systems process a large number of containers quickly and provide robust data, but they also continue to have technical problems causing downtime. The establishment of the U.S. Department of Energy (DOE) Second Line of Defense (SLD) Help Desk has assisted in resolving many maintenance and technical issues quickly and efficiently and has decreased systems and operational downtimes.

SFI scanning and imaging operations in the Port of Southampton continue to operate on a 6 days per week, 24 hours per day schedule. (b)(5), (b)(2) & (b)(7)(E)

(b)(5), (b)(2) & (b)(7)(E)

The scanning equipment that was imported into the United Kingdom and the construction of the facilities to support SFI operations in the Port of Southampton were subject to a Value Added Tax (VAT) of 17.5 percent. During the negotiations and early implementation of the pilot study, CBP requested a waiver of this tax. After extensive discussions, including letters to the office of the Prime Minister, the United Kingdom waived the VAT on imported SFI equipment, on the grounds of temporary entry to the United Kingdom, for a period of two years. The Government of the United Kingdom also waived the VAT on SFI construction because it improved the infrastructure of the port. However, when the two years end or a transfer of equipment occurs, VAT will be assessed. In 2006, Science Applications International Corporation (SAIC)

<sup>1</sup> DOE purchased a limited number of ASP detection devices and deployed a unit at Southampton as part of an ongoing effort to gain both operational experience and insight into the viability of these units as radiation detection/isotope identification devices. The ASP is undergoing a DOE field test and is not used for official adjudication of RPM alarms.

v  
~~FOR OFFICIAL USE ONLY~~

**WARNING:** This document is ~~FOR OFFICIAL USE ONLY~~. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

manifested the value of the Non-intrusive Inspection (NII) equipment (P-7500) at \$1.8 million, which obligates CBP to pay \$315,600 (17.5 percent of \$1.8 million) to the Government of the United Kingdom to satisfy the VAT. Currently, CBP is in discussions with the American Embassy and the Government of the United Kingdom on a resolution of the outstanding debt owed.

In Puerto Cortés, Honduras, SFI scanning operations continue to demonstrate the success of the SFI program in countries where the government is very supportive of this initiative. However, the operation and maintenance of the scanning system remains a unique challenge in Puerto Cortés since the NII equipment used for SFI operations was purchased separately by the Government of Honduras and in advance of the development of integrated radiation scanning systems. This adds additional challenges since the maintenance of the imaging equipment is out of the control of CBP. The scanning equipment and software continues to experience sporadic instances of downtime that are typically resolved within a few hours. However, SFI scanning operations in Puerto Cortés continue to experience instances where the (b)(2)&(b)(7)(E)

(b)(2)&(b)(7)(E)

Since May 27,

2009, (b)(2)&(b)(7)(E)

(b)(2)&(b)(7)(E)

Efforts are being made to repair the damages to the infrastructure and scanning equipment. Additionally, software issues prevented the transmission of NII data to the Central Alarm System (CAS) from the mobile NII equipment, which took over two weeks to resolve.

The current political unrest in Honduras has led to routine protests and roadblocks, which have impeded the team's ability to report for work at the port. (b)(2) (b)(7)(E)

(b)(2) (b)(7)(E)

(b)(2) (b)(7)(E)

Since June 28, 2009, the SFI team has been prevented from reporting to work on six occasions due to street protests and roadblocks. During these instances,

(b)(2)&(b)(7)(E)

(b)(2)&(b)(7)(E)

In spite of the political situation, SFI scanning operations in Puerto Cortés have not been affected and port management, as well as Honduran Customs, continues to support DHS's SFI mission.

Port Qasim, Pakistan, continues to showcase the successes of the SFI program in a country where the government is very supportive of the initiative; from constructing the scanning site to providing adequate staffing levels for SFI, the Government of Pakistan remains a strong partner.

Since the implementation of the scanning program at Port Qasim, shippers in the region are routing more containers bound for the United States through Port Qasim. CBP completed the installation of a second NII system with OCR capabilities to account for the increase in container

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

traffic, as well as to minimize the impact of NII equipment downtime by providing system redundancy. Additionally, CBP deployed (b)(2)&(b)(7)(E)

(b)(2)&(b)(7)(E)

The major challenge to SFI operations in Port Qasim continues to be the downtime of the scanning equipment (including the (b)(2)&(b)(7)(E)). The extreme climate conditions, numerous power outages, and disruptions to the communication lines and service have contributed to several instances of equipment and system down time.

Regarding the Modern Terminal in Hong Kong, following discussions on April 21, 2009 between the HKG and CBP, and a follow-up discussion between CBP and Hong Kong Trade and Industry Department executive management on April 30, 2009, both parties jointly agreed to cease maritime container scanning at the conclusion of the successful pilot period, which ended as scheduled on April 30, 2009. While the HKG had initially requested to "stand down" operations while they consulted with members of the trade on a possible extension of the pilot, both parties ultimately determined that the full value of the one-lane pilot had been realized and that there is no further purpose served by continuing operations. CBP has begun making the necessary arrangements to decommission the equipment and plan for redeployment to another location.

This pilot provided valuable operational lessons learned on the technical, logistical, and diplomatic challenges with scanning maritime containers in a high-volume port such as Hong Kong. CBP and the HKG have agreed to continue to work together under CSI and explore alternative approaches toward enhancing container and trade security through risk management and total supply chain security.

On May 16, 2009, CBP officials met representatives from SAIC and Modern Terminal (MTL) to discuss the de-commissioning of the Integrated Container Inspection System (ICIS) lane. SAIC obtained the required construction permits and assembled the equipment and personnel required to de-commission the ICIS Lane.

On July 27, 2009, a team led by CBP and SAIC traveled to Hong Kong to dismantle and crate the gamma imaging system, RPMs, OCR equipment, and computer systems. The gamma imaging radiological source will be crated and stored (b)(2)&(b)(7)(E) while the scanning equipment will be stored (b)(2)&(b)(7)(E) until deployed to a location selected by CBP. The cost to CBP to de-commission the ICIS lane is approximately \$626,500. As anticipated, CBP completed the decommissioning of the ICIS lane and has all the equipment crated and stored as of the third week of August 2009.

vii

~~FOR OFFICIAL USE ONLY~~

WARNING: This document is ~~FOR OFFICIAL USE ONLY~~. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

~~FOR OFFICIAL USE ONLY~~  
**LAW ENFORCEMENT SENSITIVE**

At the Gamman Terminal in Busan, Korea, SFI integrated scanning system is fully operational and is processing containers through the RPM equipment while truck drivers traverse the NII system on a voluntary basis. During bi-lateral discussions between CBP officials and representative from the Government of The Republic of Korea (ROK) a held in Seoul, Korea, on June 25, 2009, the ROK Government expressed their desire to extend SFI scanning operations in Busan. At the request of the ROK Government, a unique Declaration of Principles (DOP) was created to allow for SFI operations to continue at the Gamman Terminal until March 17, 2010.

In Salalah, Oman, the implementation of SFI operations in the Port of Salalah continues to progress with equipment installation and system integration. Since the last report, DOE has completed the assembly of all five Mobile Radiation Detection and Identification (MRDIS) units. (b)(2) (b)(7)(E)

(b)(2) (b)(7)(E)

On July 1, 2009, MRDIS system testing and the Shipper server installation were put on hold at the request of the port operator, pending agreed scope, timeline, and test criteria developed by DOE. DOE continues to work with the Port's Terminal Operating System (TOS) vendor to develop a link between the CAS and the Port's TOS to communicate holds on alarming containers and releases on containers when the alarm is resolved. DOE and the TOS vendor have completed the system requirements document and project the programming to be completed for December 2009 testing.

The CBP-deployed NII equipment has been operational since February 2008, which has been scanning all U.S.-bound containers identified as high-risk by the SFI team. (b)(5) (b)(2) & (b)(7)(E)

(b)(5) (b)(2) & (b)(7)(E)

CBP is providing outreach and familiarization training of SFI scanning operations to CBP officers assigned to the Advanced Targeting Unit (ATU), Anti-Terrorist-Contraband Enforcement Teams (AT-CET), and NTC-C. The outreach and familiarization training focuses on the additional container scanning and imaging data that are captured and transmitted to CBP and made available to CBP officers to utilize in conjunction with advanced manifest data (i.e.,

viii

~~FOR OFFICIAL USE ONLY~~

**WARNING:** This document is ~~FOR OFFICIAL USE ONLY~~. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

24-Hour Rule information, advance data provided by the Import Security Filings and Additional Carrier Requirements rule), Customs Trade Partnership Against Terrorism (C-TPAT) information, and the Automated Targeting System (ATS) to assess the risk of each container coming to the United States.

With respect to the SFI software enhancements, several improvements have been made in the SFI infrastructure and the CAS systems to enhance performance, reliability, and usability. These enhancements are especially relevant since they enhance our ability to efficiently manage increased message traffic in anticipation of additional SFI ports becoming operational in 2009 and beyond. These technological enhancements include implementation of a robust messaging gateway component that is capable of receiving and processing much larger volumes of electronic messages from SFI ports efficiently and securely. This gateway component seamlessly integrates with a message distribution mechanism that efficiently regulates the flow and consumption of such messages to the SFI application.

Functional improvements to the system include several features that enhance the alarm adjudication process and improve bi-directional communication between port-based personnel and U.S.-based CBP targeting and scientific services officials. In addition, these system enhancements supported a seamless integration of a second NII system at Port Qasim in Pakistan.

~~FOR OFFICIAL USE ONLY~~

<p>WARNING: This document is <del>FOR OFFICIAL USE ONLY</del>. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.</p>
--

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

## Table of Contents

I. Legislative Requirement	1
II. Background	4
III. Update of SFI Ports and Equipment	6
IV. Update of SFI Infrastructure Technology Solutions	19
V. Future Deployment Strategy	22
VI. Conclusion	24
VII. Appendix A – Acronym List	25

x

~~FOR OFFICIAL USE ONLY~~

**WARNING:** This document is ~~FOR OFFICIAL USE ONLY (FOUO)~~. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

## I. Legislative Requirement

This report is the third in a series of semi-annual updates required by Section 232(c) of the Security and Accountability For Every (SAFE) Port Act of 2006, Pub L. No. 109-347, 120 Stat. 1917 (October 13, 2006). In Section 231 of the SAFE Port Act, Congress directed the Secretary of DHS, in coordination with the Secretary of the DOE, as necessary, and the private sector and host governments when possible, to pilot an integrated scanning system at three foreign ports. Thus, this is the third report on the full-scale deployment of the integrated scanning system to capture 100 percent of U.S.-bound, maritime containers. Section 232 of the SAFE Port Act, as originally enacted, read:

**SEC. 232. SCREENING AND SCANNING OF CARGO CONTAINERS.**

**(a) ONE HUNDRED PERCENT SCREENING OF CARGO CONTAINERS AND 100 PERCENT SCANNING OF HIGH-RISK CONTAINERS.—**

**(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.*

**(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.*

**(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 subsection (b)*

1

~~FOR OFFICIAL USE ONLY~~

<p>WARNING: This document is <del>FOR OFFICIAL USE ONLY</del>. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.</p>
--

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

*and the cost of deploying the system at each foreign port at which the integrated scanning systems are deployed.*

Section 231 (c) of the SAFE Port Act, referenced above, continues to read as follows:

*SEC. 231. Pilot Integrated Scanning System.*

...  
*(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;*
- (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.*

However, on August 3, 2007, the President signed the 9/11 Act, Pub. L. No. 110-53, 121 Stat. 489. Under Title XVII of the 9/11 Act, titled Maritime Cargo, Section 1701 amended Section 232(b) of the SAFE Port Act to require 100 percent scanning of high-risk containers at all foreign ports shipping containers to the United States. The 9/11 Act establishes the following under Section 1701(a):

*SEC. 1701. CONTAINER SCANNING AND SEALS.*

*(a) CONTAINER SCANNING.—Section 232(b) of the SAFE Ports Act (6 U.S.C. 982(b)) is amended to read as follows:*

*“(b) FULL-SCALE IMPLEMENTATION.—*

*“(1) IN GENERAL.—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.*

*“(2) APPLICATION.—Paragraph (1) shall apply with respect to containers loaded on a vessel in a foreign country on or after the earlier of—*

*“(A) July 1, 2012; or*

*“(B) such other date as may be established by the Secretary under paragraph (3).*

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

*“(3) ESTABLISHMENT OF EARLIER DEADLINE.—The Secretary shall establish a date under (2)(B) pursuant to the lessons learned through the pilot integrated scanning systems established under Section 231.*

*“(4) EXTENSIONS.—The Secretary may extend the date specified in paragraph (2)(A) or (2)(B) for 2 years, and may renew the extension in additional 2-year increments, for containers loaded in a port or ports, if the Secretary certifies to Congress that at least two of the following conditions exist:*

*“(A) Systems to scan containers in accordance with paragraph (1) are not available for purchase and installation.*

*“(B) Systems to scan containers in accordance with paragraph (1) do not have a sufficiently low false alarm rate for use in the supply chain.*

*“(C) Systems to scan containers in accordance with paragraph (1) 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 in accordance with paragraph (1) cannot be integrated, as necessary, with existing systems.*

*“(E) Use of systems that are available to scan containers in accordance with paragraph (1) will significantly impact trade capacity and the flow of cargo.*

*“(F) Systems to scan containers in accordance with paragraph (1) do not adequately provide an automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel.*

~~FOR OFFICIAL USE ONLY~~

<p>WARNING: This document is <del>FOR OFFICIAL USE ONLY</del>. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.</p>
--

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

## II. Background

DHS and DOE, along with 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.

On October 13, 2006, President George W. Bush signed into effect the SAFE Port Act. The purpose of the SAFE Port Act is to improve maritime and cargo security through enhanced layered defenses, including hardening critical infrastructure, increasing port defenses against possible attacks, and increasing 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.

The SAFE Port Act also codified a number of supply chain security programs that DHS established following the September 11, 2001, terrorist attacks (programs that continue today). Specifically, the SAFE Port Act statutorily established DHS's advanced information requirements and automated analysis, programs such as the Customs-Trade Partnership Against Terrorism (C-TPAT) and CSI, and the use of NII technology to scan high-risk shipments. The inclusion of these provisions reflects the SAFE Port Act's support for the current layered, risk-based approach to maritime and cargo security.

These programs form the backbone of DHS's risk-management, 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 this strategy is that it ensures continuous security at multiple nodes in the supply chain by distributing resources so that one threat does not overshadow other vulnerable areas that could also be exploited.

SFI represents yet another component of this layered enforcement strategy for protecting the Nation. SFI, through partnerships with foreign governments, terminal operators, and carriers, enhances DHS's capability to better assess the security of U.S.-bound maritime containers by scanning them for special nuclear and other radioactive materials before they are laden on

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

vessels bound for the United States. An integrated scanning system, consisting of an RPM provided by DOE and NII equipment provided by CBP, collects and aggregates container data. The data are then linked to the associated container using OCR technology and analyzed by CBP officers who determine if the container should be referred to the host Nation for secondary examination prior to lading.

Meeting the legislative requirements of the SAFE Port Act, the first three SFI ports (Puerto Cortés, Honduras; Port Qasim, Pakistan; and Southampton, United Kingdom) became fully operational on October 12, 2007, and are now attempting to scan all U.S.-bound maritime containers. DHS and DOE also deployed scanning equipment to Salalah (Oman), Port Busan (ROK), and a terminal in Hong Kong. SFI sought partnerships in these locations because they present a unique set of challenges and provide diverse environments in which to evaluate varying options.

**Report Methodology**

This report is based upon data collected during initial negotiations, systems installations and initial testing, and full SFI 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.

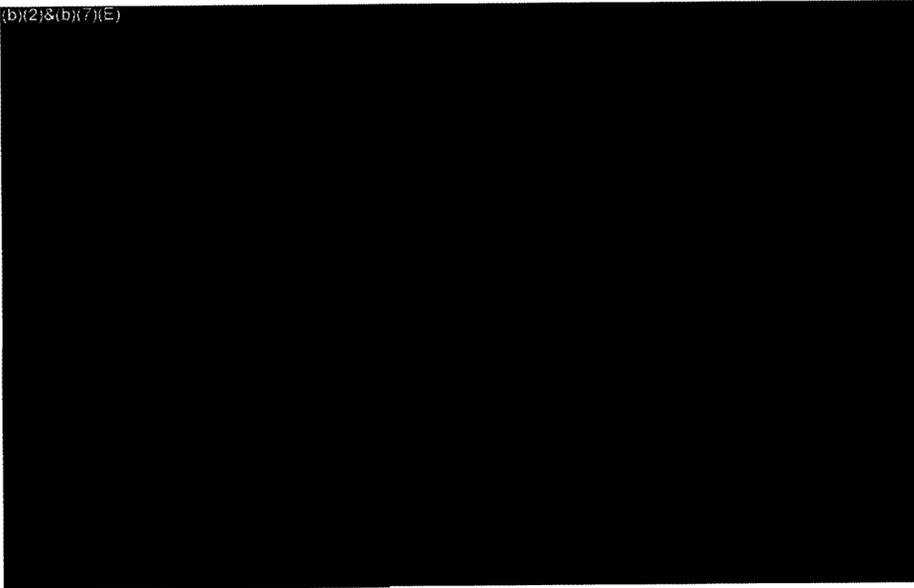
<p>WARNING: This document is <del>FOR OFFICIAL USE ONLY</del>. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.</p>
--

### III. Update of SFI Ports and Equipment

The following section provides an update to the last Congressional report on the developments and operation of SFI in each port.

#### Southampton, United Kingdom

Figure 1-1 Layout of SFI Scanning System, Port of Southampton



As indicated in the previous reports, implementation and operation of the SFI scanning process did not significantly impede the flow of container traffic, nor has it resulted in traffic bottlenecks within the terminal. This continues to be the case, with the Southampton Container Terminal reporting little or no negative effects as a result of SFI operations.

Previous reports have highlighted key issues/changes to the SFI scanning and imaging operations at the Port of Southampton since the pilot study was implemented. A few issues/changes are worth reiterating in this report. First, Her Majesty's Revenue and Customs (HMRC) ended their participation in the SFI program after the completion of the pilot in April 2008. Therefore, HMRC does not staff the SFI site in Southampton and elected to revert back to CSI protocols that were agreed to in December 2002. Currently, CBP officers stationed at the Port of Southampton (b)(2)&(b)(7)(F)

(b)(2)&(b)(7)(E)

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

Second, CBP has successfully transferred the in-country targeting responsibilities of the SFI team to (b)(2)&(b)(7)(E)

(b)(2)&(b)(7)(E)

Finally, a technical solution for scanning transshipment and railhead containers in Southampton has yet to be developed. U.S.-bound transshipped containers 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. As such, they do not pass through the pre-gate area and the SFI scanning systems. During the SFI installation planning process, the Southampton Container Terminal 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.

Equipment and system downtime continue to be a challenge for SFI scanning operations at the Port of Southampton, although the SFI program has seen improvements since the last report submitted to Congress on March 17, 2009. The ASP and the imaging system are some of the newest technologies deployed at any port.<sup>2</sup> These systems process a large number of containers quickly and provide robust data, but they also continue to have technical problems causing downtime. The establishment of DOE's SLD Help Desk has helped to resolve many maintenance and technical issues quickly and efficiently. The purpose of the Help Desk is to provide partner countries with a pathway to gain access to the technical expertise available from the SLD system providers and the DOE National Laboratories. It serves as a single point of contact for partner countries to access technical support for the timely resolution of problems associated with the SLD radiation detection systems that have been installed throughout the world and at SFI ports. The technical support provides the timely resolution of problems associated with the SLD radiation detection systems and has resulted in a decrease of systems and operational downtimes.

SFI scanning and imaging operations in the Port of Southampton continue to operate on a 6 days per week, 24 hours per day schedule (b)(2)&(b)(7)(E)

(b)(2)&(b)(7)(E)

<sup>2</sup> DOE purchased a limited number of ASP detection devices and deployed a unit at Southampton as part of an ongoing effort to gain both operational experience and insight into the viability of these units as radiation detection/isotope identification devices. The ASP is undergoing a DOE field test and is not used for official adjudication of RPM alarms.

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

(b)(5), (b)(2) & (b)(7)(E)

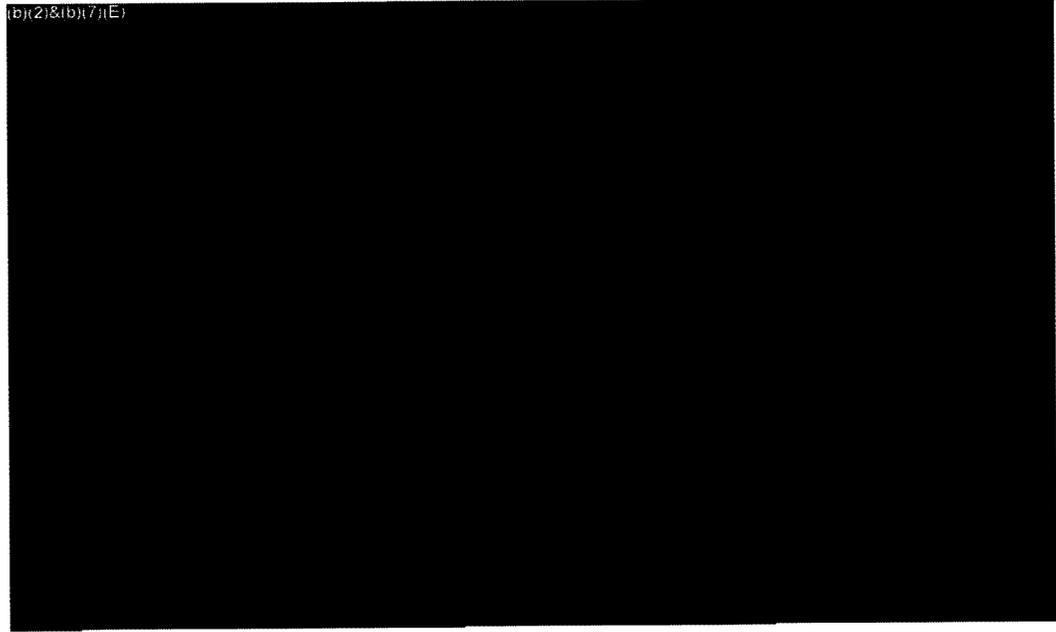


The scanning equipment that was imported into the United Kingdom and construction of the facilities to support SFI operations in the Port of Southampton were subject to a VAT of 17.5 percent. During the negotiations and early implementation of the pilot study, CBP requested a waiver of this tax. After extensive discussions, including letters to the office of the Prime Minister, the United Kingdom waived the VAT on imported SFI equipment, on the grounds of temporary entry to the United Kingdom, for a period of two years. The Government of the United Kingdom also waived the VAT on SFI construction because it improved the infrastructure of the port. However, when the two years end or a transfer of equipment occurs, the VAT will be assessed. In 2006, SAIC manifested the value of the NII equipment (P-7500) at \$1.8 million, which obligates CBP to pay \$315,000 (17.5 percent of \$1.8 million) to the Government of the United Kingdom to satisfy the VAT. Currently, CBP is in discussions with the American Embassy and the Government of the United Kingdom on a resolution of the outstanding debt owed.

**Puerto Cortés, Honduras**

**Figure 1-2 Layout of SFI Scanning System, Puerto Cortés**

(b)(2)&(b)(7)(E)



~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

Puerto Cortés remains an active and valuable SFI port and provides an opportunity to deploy scanning equipment in a port with a higher volume of containers and with little or no transshipment. However, the availability of advanced electronic data remains one of the major challenges for the SFI program in Puerto Cortés. The terminal operator in Puerto Cortés has limited advance electronic data available, and containers may arrive days in advance of departure. Manifest and other data elements under the Importer Security Filing and Advanced Carrier Requirement rule are received by CBP only 24 hours in advance of departure. Therefore, if a container arrives at the port gate days in advance of it being loaded onto the vessel, the advance data will not yet have been submitted to CBP or the port and the container may still proceed through the scanning equipment. 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 data is later validated once CBP receives the 24-hour rule information. This process is very labor intensive and has not yet been remedied. (b)(2)&(b)(7)(E)

(b)(2)&(b)(7)(E)

The operation and maintenance of the scanning system remains a challenge at all SFI ports; however, Puerto Cortés is unique in that the NII equipment used for SFI operations was purchased separately by the Government of Honduras and in advance of the development of integrated radiation scanning systems. This adds additional challenges since the maintenance of the imaging equipment is out of CBP's control. The scanning equipment and software continue to experience sporadic instances of downtime that are typically resolved within a few hours.

However, SFI scanning operations in Puerto Cortés continue to experience instances where the

(b)(2)&(b)(7)(E) Since May 27, 2009, the  
(b)(2)&(b)(7)(E)  
(b)(2)&(b)(7)(E)

Efforts are being made to repair the damages to the infrastructure and scanning equipment. Additionally, software issues prevented the transmission of NII data to the CAS from the mobile NII equipment, which took over two weeks to resolve.

(b)(5), (b)(2) & (b)(7)(E)

**WARNING:** This document is ~~FOR OFFICIAL USE ONLY~~. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

~~FOR OFFICIAL USE ONLY~~  
**LAW ENFORCEMENT SENSITIVE**

Coup d'etat: On June 28, 2009, Honduran President Manuel Zelaya was seized by soldiers, acting on the orders of the Honduran Supreme Court, and sent to exile in Costa Rica. Following President Zelaya's removal, the Honduran National Congress approved Roberto Micheletti as the interim President until the November presidential elections. Latin American nations, as well as the United States and several other European nations, have publicly condemned the forced removal of Zelaya.

As a result of the current political situation, the SFI team has experienced new challenges. The civil unrest has led to routine protests and roadblocks which impede the team's ability to report for work at the port. (b)(2) (b)(7)(E)

(b)(2) (b)(7)(E)

(b)(2) (b)(7)(E)

Since June 28, 2009, the SFI team has been prevented from reporting to work on six occasions due to street protests and roadblocks. During these instances,

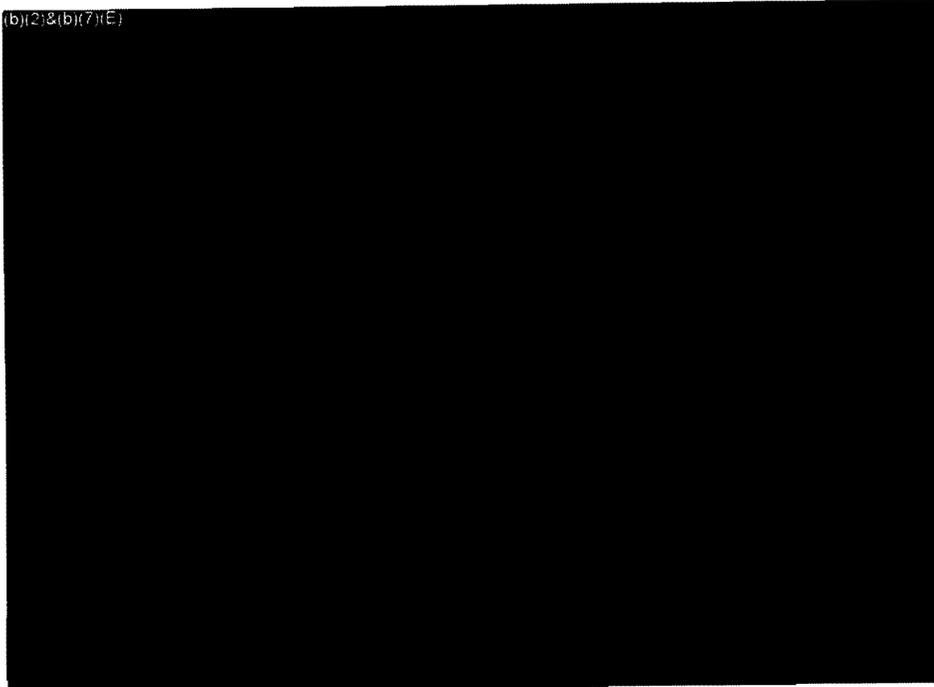
(b)(2)&(b)(7)(E)

(b)(2)&(b)(7)(E) in spite of the political situation, SFI scanning operations in Puerto Cortés have not been affected and port management, as well as Honduran Customs, continue to support DHS's SFI mission.

~~FOR OFFICIAL USE ONLY~~  
**LAW ENFORCEMENT SENSITIVE**

**Qasim, Pakistan**

**Figure 1-3 Layout of SFI Scanning System, Port Qasim**



Port Qasim continues to showcase the successes of the SFI program in a country where the government is very supportive of the initiative; from constructing the scanning site to providing adequate staffing levels for SFI, the Government of Pakistan remains a strong partner in deploying SFI operations to scan all U.S.-bound maritime containers.

Port Qasim presents 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 FSNs hired and vetted by the U.S. Consulate General in Karachi. At all times, CBP officers use live video feeds streaming directly from Pakistan to the United States to monitor SFI operations in Port Qasim, including physical examinations of the containers. Creating the process for real-time data transmission and analysis required the development, installation, and integration of new software.

Operations in Port Qasim show that the flow of commerce has not been impacted by SFI operations. In fact, since SFI became operational, Port Qasim has experienced an increase in the container volume of exports to the United States and that trend has continued.

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

CBP has installed an additional NII system with OCR capabilities to Port Qasim to account for the increase in container traffic and to minimize the impact of NII equipment downtime by providing system redundancy. (b)(2)&(b)(7)(E)

(b)(2)&(b)(7)(E)

The major challenge to SFI operations in Port Qasim continues to be the downtime of the scanning equipment (including (b)(2)&(b)(7)(E)). The extreme climate conditions, numerous power outages, and disruptions to the communication lines and service have contributed to several instances of equipment and system down time.

**Hong Kong (Modern Terminal)**

**Figure 1-4 Hong Kong ICIS Configuration**

(b)(2)&(b)(7)(E)

Following discussions on April 21, 2009, between the HKG and CBP, and a follow-up discussion between CBP and Trade and Industry Department executive management on April 30, 2009, both parties jointly agreed to cease maritime container scanning at the conclusion of the successful pilot period, which ended as scheduled on April 30, 2009. While the HKG had initially requested to "stand down" operations while they consulted with members of the trade on a possible extension of the pilot, both parties ultimately determined that the full value of the one-lane pilot had been realized and that there is no further purpose served by continuing operations. CBP has begun making the necessary arrangements to decommission the equipment and plan for redeployment to another location.

~~FOR OFFICIAL USE ONLY~~

WARNING: This document is ~~FOR OFFICIAL USE ONLY~~. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

This pilot provided valuable operational lessons learned on the technical, logistical, and diplomatic challenges with scanning maritime containers in a high-volume port such as Hong Kong. CBP and the HKG have agreed to continue to work together under CSI and explore alternative approaches toward enhancing container and trade security through risk management and total supply chain security.

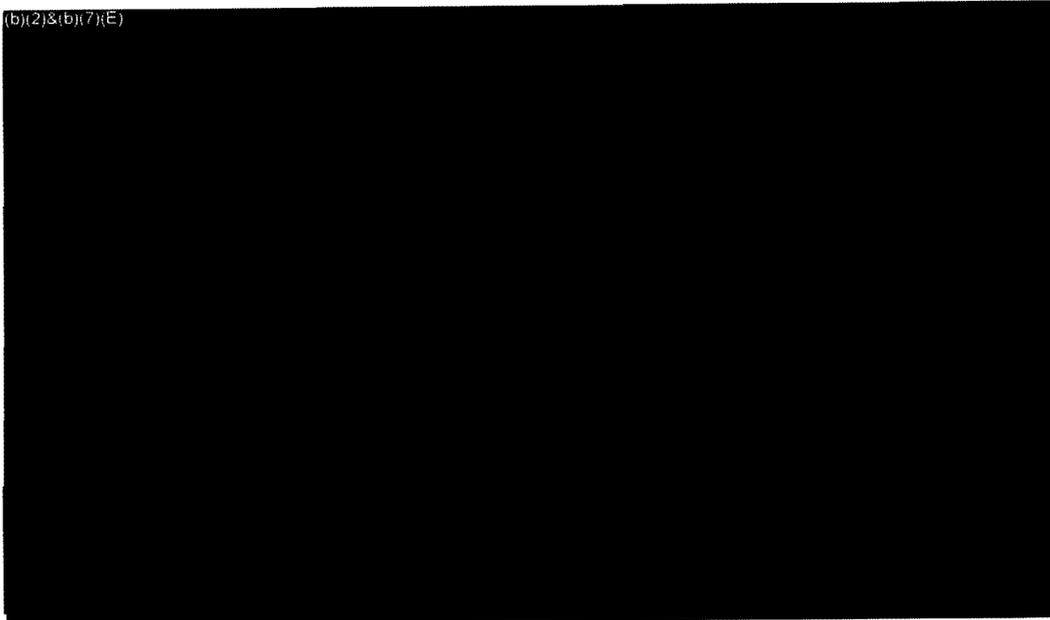
On May 16, 2009, CBP officials met representatives from SAIC and MTL to discuss the de-commissioning of the ICIS lane. SAIC obtained the required construction permits and assembled the equipment and personnel required to de-commission the ICIS Lane.

On July 27, 2009, a team led by CBP and SAIC traveled to Hong Kong to dismantle and crate the gamma imaging system, RPM, OCR equipment, and computer systems. The gamma imaging radiological source will be crated and stored (b)(2)&(b)(7)(E) while the scanning equipment will be stored (b)(2)&(b)(7)(E). The cost to CBP to de-commission the ICIS lane is approximately \$626,500. As anticipated, CBP completed the decommissioning of the ICIS lane and has all the equipment crated and stored as of the third week of August 2009.

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

**Busan, Korea (Gamman Terminal)**

**Figure 1-5 Layout of SFI Scanning System, Busan**



As identified in previous reports, the health and safety concerns expressed by the trucker unions regarding the drive-through NII systems remain a chief concern. The U.S. Government has taken several steps to assure all concerned parties that the NII system poses no harm to the health and safety of the drivers and operators. CBP and the NII vendor, SAIC, have provided briefings to the unions and all interested government personnel regarding the safety of the NII equipment. Additionally, the Korean Institute for Nuclear Safety completed a study of the system and certified the NII equipment as safe to use in Busan. Finally, to allay remaining health and safety concerns, the U.S. Government purchased and installed a radiation monitoring system to notify all drivers of the minimal radiation exposure levels. These additional steps secured an agreement between the U.S. and South Korean Governments to allow full operations of the SFI integrated scanning system. An agreement was reached and full scanning operations commenced on March 18, 2009, with the SFI integrated scanning system processing containers through the RPM equipment while truck drivers traverse the NII system on a voluntary basis.

During bi-lateral discussions between CBP officials and representatives from the ROK Government held in Seoul, Korea, on June 25, 2009, the ROK Government expressed their desire to extend SFI scanning operations in Busan. At the request of the ROK Government, a unique DOP was created to allow for SFI operations to continue at the Gamman Terminal until March 17, 2010.

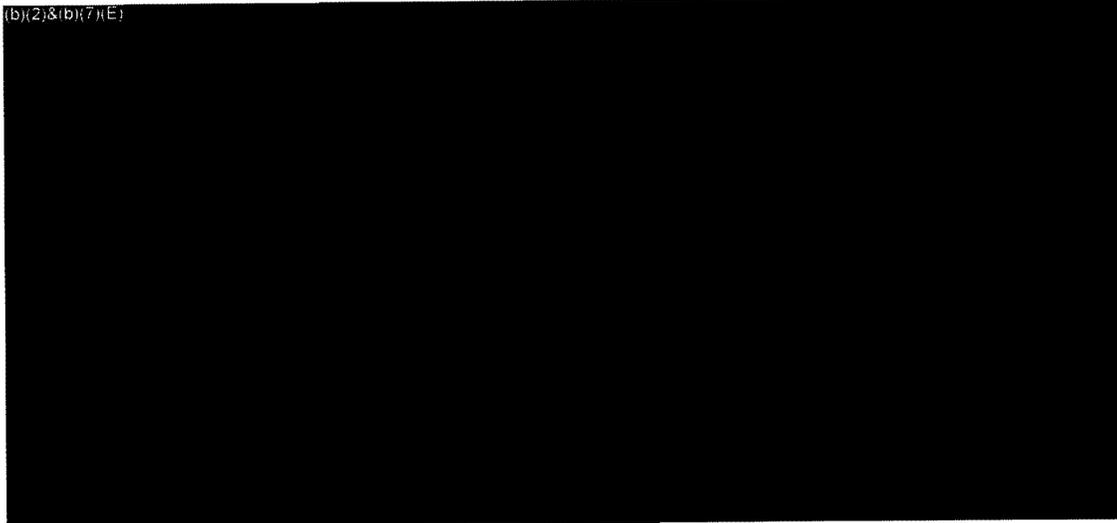
~~FOR OFFICIAL USE ONLY~~

**WARNING:** This document is ~~unclassified~~. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOI information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

Salalah, Oman

**Figure 1-6 Layout of SFI Scanning System, Port of Salalah**



The implementation of SFI operations in the Port of Salalah, Oman, continues to progress with equipment installation and system integration. Since the last report, DOE has completed the assembly of all five MRDIS units. During a controlled exercise of scanning containers with the primary MRDIS units, (b)(7)(E)

(b)(7)(E)

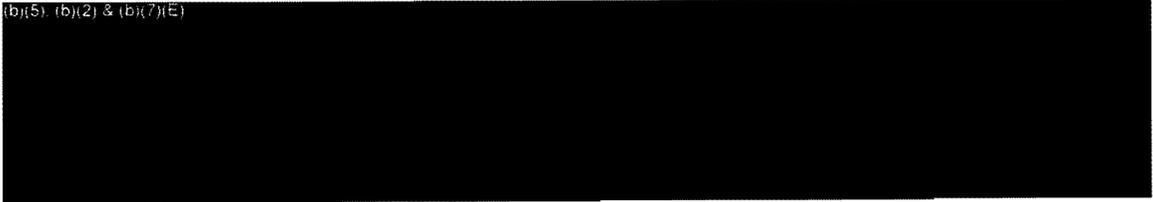
On July 1, 2009, MRDIS system testing and the Shipper's server installation were put on hold at the request of the port operator, pending agreed scope, timeline, and test criteria developed by DOE.

DOE continues to work with the Port's TOS vendor to develop a link between the CAS and the Port's TOS to communicate holds on alarming containers and releases on containers when the alarm is resolved. DOE and the TOS vendor have completed the system requirements document and project the programming to be completed for December 2009 testing.

The CBP-deployed NII equipment has been operational since February 2008 and remains available to scan all U.S.-bound containers identified as high-risk by the SFI team. Based on recommendations from the Omani government, and with the concurrence of the Salalah Port

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

(b)(5), (b)(2) & (b)(7)(E)



CBP has increased the staffing at Port Salalah by hiring three FSNs to support the SFI scanning and imaging operations. The FSNs have undergone training, to include port operations, systems familiarity, and an English class, and will be instrumental in facilitating communication between the port and U.S. Government officials.

**SFI Outreach and Familiarization Training for Domestic Seaports**

CBP is providing outreach and familiarization training of SFI scanning operations to CBP officers assigned to the ATUs, AT-CET, and NTC-C. The outreach and familiarization training focuses on the additional container scanning and imaging data that are captured and transmitted to CBP and made available to CBP officers to utilize in conjunction with advanced manifest data (i.e., 24-Hour Rule information, advance data provided by the Import Security Filings and Additional Carrier Requirements rule), C-TPAT information, and the ATS to assess the risk of each container coming to the United States.

**Updated Cost of SFI Operations**

The table on the next page lists the expenditures by DHS and DOE on the pilot ports since the inception of the SFI program. The numbers are current through July 31, 2009, and reflect actual costs to that point.

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

DHS and DOE Expenditures on Pilot Ports

Element	DHS Cost	DOE Cost <sup>3</sup>
Cables	\$2,165,940	
Travel	\$3,251,802	\$237,454
Equipment	\$15,500,000	\$5,663,490
Contract Modifications	\$1,195,000	
Software development	\$18,159,995	
Training	\$231,502	\$3,546,261
Site Survey	\$200,000	
Program Office Support (contractor)	\$2,020,830	
Software licenses	\$628,486	
Hardware Server Licenses	\$82,132	
Government staffing	\$4,053,728	
Installation		\$23,135,023
Communications	\$2,554,858	\$6,766,421
Testing	\$26,000	\$1,182,470
Maintenance		\$2,864,571
<b>TOTAL</b>	<b>\$50,070,273</b>	<b>\$43,395,690</b>

The following is a description of the above cost elements:

Cables – “Fund Cite Cables” are used to release funds overseas. These funds may be used to build structures in support of SFI operations, allow for purchase of office equipment, or cover any other expense incurred abroad to support the SFI program operations, including salaries of FSNs hired at SFI locations.

Travel – This category pertains to travel associated with the negotiations, deployment, and operations of scanning systems as well as SFI TDY staff relocation overseas and travel.

Equipment – This category pertains to DHS and DOE-provided equipment in support of SFI operations (i.e., NII, RPMs, ASP, OCR, and MRDIS).

<sup>3</sup> DOE costs are current through June 30, 2009. Since the last report to Congress, DOE has reconciled estimated costs with actual costs, which has reduced the entries for equipment and installation.

~~FOR OFFICIAL USE ONLY~~  
**LAW ENFORCEMENT SENSITIVE**

Contract Modifications – This category pertains to any modifications to initial equipment installation contracts that resulted in additional costs.

Software Development – This category pertains to funding allocated to the CBP Office of Information and Technology to develop and maintain all software required to process the data collected by the SFI equipment and the transmission of this data to the ATS system. It also includes the development of the SFI interface and any additional developments required.

Training – This category includes any vendor-provided training required to operate SFI equipment and conduct SFI-related duties. DOE also trains those individuals in the host country who will be responsible for operating and maintaining the equipment.

Site Survey – This is the cost incurred by contractors to develop and document initial assessments at each candidate port in preparation for SFI implementation. (Note: DOE site survey costs are captured in the Installation line.)

Program Office Support – These funds were expended to develop the Program Office organization and prepare documentation according to CBP-approved program life-cycle process (contractor support).

Software Licenses – This category pertains to the cost of software licenses for all applications required to successfully operate SFI.

Hardware Server License – This category addresses the cost of licenses required to operate servers.

Government Staffing – This includes salary expenses for staff permanently assigned to Headquarters as well as the cost of TDY staff assigned to the SFI project at Headquarters and the cost of maintaining U.S. Government employees (TDY or permanent) at SFI locations.

Installation – This category includes DOE costs associated with the installation and integration of radiation detection equipment and related communication systems.

Communications – This category includes costs associated with providing the associated communications system for the scanning equipment and transfer of scanning data, including CAS hardware and software development costs incurred by DOE.

Testing – This category includes the cost of testing DOE's radiation detection equipment and associated communications system before it is turned over to the host country for operation.

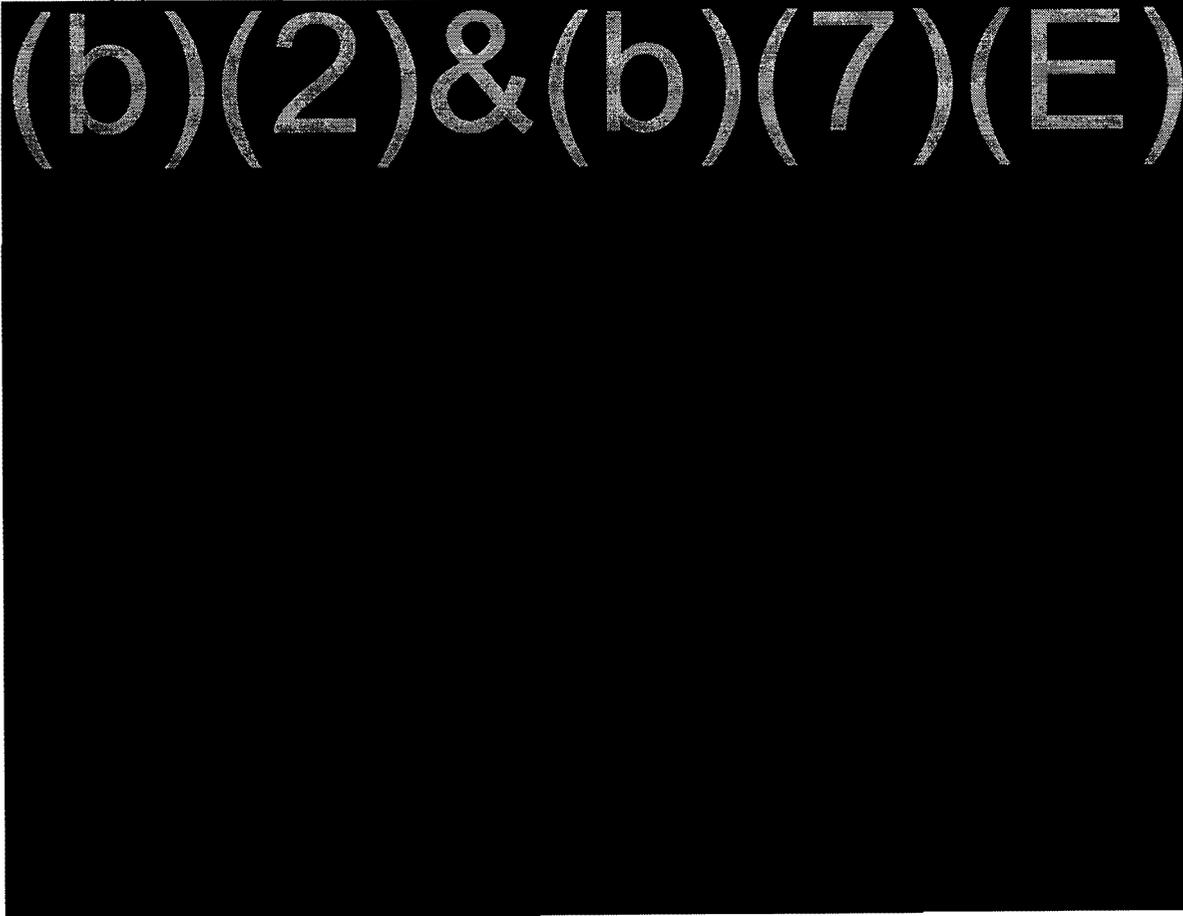
Maintenance – This category includes the cost of DOE-provided maintenance on DOE installed equipment and systems.

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

## IV. Update of SFI Infrastructure Technology Solutions

### SFI Software

As noted in the previous report, CBP has developed a software system to facilitate the collection, analysis, and reporting of images and related data captured during the examination of U.S.-bound containers at SFI pilot ports. This software system, (b)(2)&(b)(7)(E)



Since the last report submitted on March 17, 2009, several improvements have been made in the SFI infrastructure and the CAS systems to enhance performance, reliability, and usability. These enhancements are especially relevant since they enhance our ability to efficiently manage increased message traffic in anticipation of additional SFI ports becoming operational in 2009 and beyond. These technological enhancements include implementation of a robust messaging gateway component that is capable of receiving and processing much larger volumes of XML

~~FOR OFFICIAL USE ONLY~~  
**LAW ENFORCEMENT SENSITIVE**

messages from SFI ports efficiently and securely. This gateway component seamlessly integrates with a message distribution mechanism that efficiently regulates the flow and consumption of such messages to the SFI application.

Functional improvements to the system include several features that enhance the alarm adjudication process and improve bi-directional communication between port based personnel and U.S.-based CBP targeting and scientific services officials. In addition, these system enhancements supported a seamless integration of a second NII system at Port Qasim, Pakistan.

As the SFI locations continue to identify challenges and present opportunities for enhancements, software modifications and technical improvements will be developed in the ATS-SFI system. These enhancements will supplement and complement the robust layered approach to container security that CBP currently applies.

**Image Anomaly Identification Software**

(b)(2)&(b)(7)(E)

(b)(2)&(b)(7)(E)

WARNING: This document is ~~FOR OFFICIAL USE ONLY (FOUO)~~. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

(b)(2)&(b)(7)(E)

Not only is the development of such software imperative to future deployments of SFI operations, but it is also required by the 9/11 Act. According to Section 1701 of the 9/11 Act, one of the statutory conditions that must exist is an "automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel."

~~FOR OFFICIAL USE ONLY~~

WARNING: This document is ~~FOR OFFICIAL USE ONLY~~. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

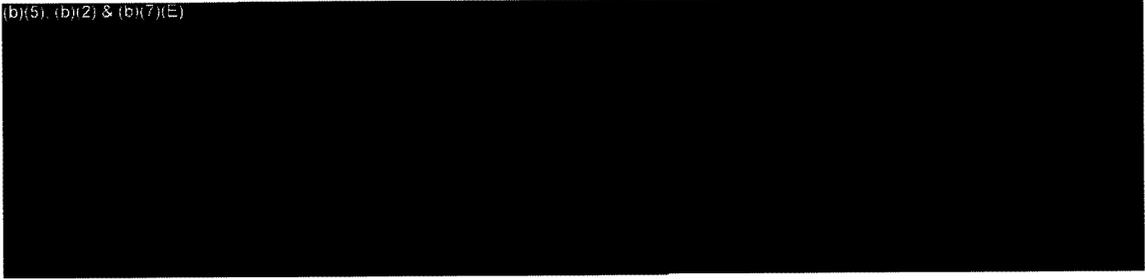
~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

## V. Future Deployment Strategy

CBP has learned some significant lessons from the initial SFI pilots in United Kingdom, Honduras, Pakistan, and from the more limited operations in the three other locations. While work continues to address the complex financial, logistical, diplomatic, and technical challenges, 100 percent scanning by 2012 will be difficult to achieve based on what we know today.

However, DHS is confident that the scan data from these systems can enhance the security of containers moving through a few strategic locations. CBP and DOE will work with specific foreign governments to develop SFI partnerships that will complement the current risk-based approach to security.

(b)(5), (b)(2) & (b)(7)(E)



~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

## VI. 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 extremely impractical and detrimental to our own economy, the economies of our trading partners, as well as the global economy. Instead, DHS relies 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 approach reduces the likelihood of a successful exploitation of any one layer in the supply chain system as a whole. The appropriate distribution of resources, based on informed judgment regarding the totality of dangers facing the Nation, is necessary 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 areas of vulnerability.

That is why it remains critical to continue to evaluate the SFI program to determine the best method to employ SFI within DHS's risk-based methodology. This report serves as an update on the ongoing effort to best understand the operational realities of SFI. Issues of cost, political will, and equipment downtime continue to present challenges. The international and industrial communities still remain largely opposed to 100 percent scanning, and have conducted studies of their own to demonstrate the negative impacts of such an effort. In light of the considerable concern expressed by many foreign and industry partners on this issue, garnering host government support for deploying scanning systems is a delicate task. However, by focusing deployments on strategic locations, DHS believes that the U.S. Government's approach to maritime security will be clearly articulated and easily understood by our trading partners as a benefit to the global economy.

Prioritizing future developments to locations of strategic importance allows DHS to most effectively allocate resources, both capital and personnel. Working with host governments and terminal operators to place radiation detection and imaging equipment in ports with a greater share of high-risk cargo will certainly complement an already successful approach to maritime security. DHS, in partnership with DOE, must continue work to refine future deployments in a viable and responsible manner. It will be critical to keep operations in current SFI locations, test new technology, and work to find solutions to complex challenges, such as transshipped containerized cargo.

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

## VII. Appendix A – Acronym List

9/11 Act	Implementing Recommendations of the 9/11 Commission Act of 2007
AT-CET	Anti-Terrorist-Contraband Enforcement Team
ATS	Automated Targeting System
ATU	Advanced Targeting Unit
ASP	Advanced Spectroscopic Portal
CAS	Central Alarm System
CBP	U.S. Customs and Border Protection
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership Against Terrorism
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
DOP	Declaration of Principles
DOS	U.S. Department of State
FSN	Foreign Service National
FY	Fiscal Year
HMRC	Her Majesty's Revenue and Customs (United Kingdom)
ICE	U.S. Immigration and Customs Enforcement
ICIS	Integrated Container Inspection System
LES	Locally Engaged Staff
MI	Megaports Initiative
MRDIS	Mobile Radiation Detection and Identification
MT	Modern Terminal
NII	Non-intrusive Inspection
NTC-C	National Targeting Center-Cargo
OCR	Optical Character Recognition
ROK	Republic of Korea

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

RPM	Radiation Portal Monitor
SAFE Port Act	Security and Accountability for Every Port Act of 2006
SAIC	Science Applications International Corporation
SFI	Secure Freight Initiative
SLD	Second Line of Defense
TDY	Temporary Duty
TRA	Telecommunication Regulatory Authority
VAT	Value Added Tax

~~FOR OFFICIAL USE ONLY~~

WARNING: This document is ~~FOR OFFICIAL USE ONLY~~. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.