



# governmentattic.org

*"Rummaging in the government's attic"*

Description of document: Copies of responses to Congressional Committees from the Department of Homeland Security (DHS)  
January 2012 - April 2013

Request date: 20-April-2013  
Request date: 21-October-2013

Released date: 03-February-2014  
Released date: 27-February-2014  
Released date: 27-April-2014  
Released date (TSA): 14-April- 2015

Posted date: 04-May-2015  
Update posted: 29-September-2015

Note: TSA records released 14-April- 2015 start PDF page 113

Source of document: FOIA Officer  
The Privacy Office  
U.S. Department of Homeland Security  
245 Murray Lane SW  
STOP-0655  
Washington, D.C. 20528-0655  
Fax: 202-343-4011  
E-mail: [foia@hq.dhs.gov](mailto:foia@hq.dhs.gov)  
[Online FOIA Request Submission Form](#)

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.



Homeland  
Security

February 4, 2014

**SENT VIA EMAIL:**

Re: **2013-HQFO-00590**

This is the final response to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated April 20, 2013, and received by this office on April 23, 2013. You are seeking a copy of each written response or letter from the Department of Homeland Security to a Congressional Committee (not a congressional office) (or Committee Chair) in calendar years 2012 and 2013 to date. By this, you mean one-time type responses to Committee inquiries, excluding from the scope of this request regular periodic reports and constituent responses to a congressional office.

In your September 30, 2013 email to this office, you agreed to a copy of each written response or letter from the Department of Homeland Security to any of the following Members of Congress in calendar years 2011, 2012 and 2013 to date: Rep. Michael McCaul, Rep. Candice Miller, Rep. Peter King, Rep. Patrick Meehan, Rep. Susan Brooks, Rep. Jeffrey Duncan, and Rep. Richard Hudson.

A search of the Enterprise Correspondence Tracking System (ECT) for documents responsive to your request produced a total of 78 pages. Of those pages, I have determined that 63 pages of the records are releasable in their entirety, and 15 pages are partially releasable pursuant to Title 5 U.S.C. § 552 (b)(5), (b)(6), and (b)(7)(E), FOIA Exemptions 5, 6 and 7(E).

FOIA Exemption 5 protects from disclosure those inter- or intra-agency documents that are normally privileged in the civil discovery context. The three most frequently invoked privileges are the deliberative process privilege, the attorney work-product privilege, and the attorney-client privilege. After carefully reviewing the responsive documents, I determined that portions of the responsive documents qualify for protection under the Deliberative Process Privilege. The deliberative process privilege protects the integrity of the deliberative or decision-making processes within the agency by exempting from mandatory disclosure opinions, conclusions, and recommendations included within inter-agency or intra-agency memoranda or letters. The release of this internal information would discourage the expression of candid opinions and inhibit the free and frank exchange of information among agency personnel.

FOIA Exemption 6 exempts from disclosure personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a balancing of

the public's right to disclosure against the individual's right to privacy. The privacy interests of the individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

Exemption 7(E) protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

Additionally, a search of the Enterprise Correspondence Tracking System (ECT) for documents responsive to your request produced an additional 328 pages. Upon review of those records, I have determined that several workflows that you are seeking are under the purview of other components. Therefore, I am referring these documents to the appropriate components for processing and direct response to you.

Customs and Border Protection (CBP) FOIA Officer, Sabrina Burroughs, for processing and direct response to you. You may contact that office in writing at U.S. Customs and Border Protection; 1300 Pennsylvania Ave., NW, Mint Annex; Washington, D.C. 20229-1181 or via telephone at 202-325-0150.

Federal Emergency Management Agency (FEMA) FOIA Officer, Terry Cochran, for processing and direct response to you. You may contact that office in writing at Federal Emergency Management Agency, 1800 South Bell Street, Mail Stop 3005, Arlington, VA 20598-3005 or via telephone at 202-646-3323.

Office of Intelligence and Analysis (I&A) FOIA Officer, Priscilla Waters, for processing and direct response to you. You may contact that office in writing at U.S. Department of Homeland Security; Office of Inspector General; Mail Stop 0305; 245 Murray Lane, SW; Washington, D.C. 20528-0305 or via telephone at 202-254-4001.

U.S. Immigration and Customs Enforcement (ICE) FOIA Officer Catrina Pavlik-Keenan, for processing and direct response to you. You may contact that office in writing at U.S. Immigration and Customs Enforcement, Freedom of Information Act Office, 500 12<sup>th</sup> Street SW, Stop 5009, Washington, D.C. 20536-5009 or via telephone at 202-732-0600, or 866-633-1182.

National Protection and Programs Directorate (NPPD) Acting FOIA Officer for NPPD, Sandy Ford Page, for processing and direct response to you. You may contact that office in writing at U.S. Department of Homeland Security, National Protection and Programs Directorate, Washington, D.C. 20528, [nppd.foia@dhs.gov](mailto:nppd.foia@dhs.gov), or via telephone at 703-235-2211.

Science and Technology Directorate (S&T) FOIA Officer for S&T, Katrina Hagan, for processing and direct response to you. You may contact that office in writing at U.S. Department of Homeland Security, Science and Technology Directorate, Washington, D.C. 20528 or via telephone at 202-254-6819.

Transportation Security Administration (TSA) FOIA Officer, Yvonne Coates, for processing and direct response to you. You may contact that office in writing at Transportation Security

Administration, TSA-20; 601 S. 12<sup>th</sup> Street; 11<sup>th</sup> Floor, East Tower; Arlington, VA 20598-6020 or via telephone at 1-866-FOIA-TSA or 571-227-2300.

U.S. Coast Guard (USCG) FOIA Officer for USCG, Gaston Brewer, for processing and direct response to you. You may contact that office in writing at U.S. Coast Guard, Commandant (CG-611); 2100 2<sup>nd</sup> Street, S.W.; Attn: FOIA Coordinator; Washington, D.C. 20593-0001 or via telephone at 202-475-3522.

U.S. Citizenship and Immigration Services (USCIS) Jill Eggleston, for processing and direct response to you. You may contact that office in writing at U.S. Citizenship and Immigration Services; National Records Center, FOIA/PA Office; P.O. Box 648010; Lee's Summit, MO 64064-8010 or via telephone at 800-375-5283.

You have a right to appeal the above withholding determination. Should you wish to do so, you must send your appeal and a copy of this letter, within 60 days of the date of this letter, to: Associate General Counsel (General Law), Mailstop 0655, U.S. Department of Homeland Security, Washington, D.C. 20528, following the procedures outlined in the DHS regulations at 6 C.F.R. § 5.9. Your envelope and letter should be marked "FOIA Appeal." Copies of the FOIA and DHS regulations are available at [www.dhs.gov/foia](http://www.dhs.gov/foia).

The Office of Government Information Services (OGIS) also mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. If you are requesting access to your own records (which is considered a Privacy Act request), you should know that OGIS does not have the authority to handle requests made under the Privacy Act of 1974. If you wish to contact OGIS, you may email them at [ogis@nara.gov](mailto:ogis@nara.gov) or call 1-877-684-6448.

Provisions of the FOIA allow us to recover part of the cost of complying with your request. In this instance, because the cost is below the \$14 minimum, there is no charge. 6 CFR § 5.11(d)(4).

If you need to contact our office again about this matter, please refer to **2013-HQFO-00590**. This office can be reached at 866-431-0486 or 202-343-1743.

Sincerely,

A handwritten signature in black ink that reads "Eric Neuschaefer". The signature is written in a cursive, flowing style.

Eric Neuschaefer  
FOIA Program Specialist

Enclosure(s): Responsive Documents, 78 pages

**MAY 25 2011**



**Homeland  
Security**

The Honorable Peter T. King  
Chairman  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your recent letter to Secretary Napolitano regarding the implementation of the REAL ID Act. I assure you the Department of Homeland Security (DHS) is committed to helping states meet the security standards of REAL ID. Although you may be disappointed with the pace of implementation by states, real progress is being made in enhancing the security of state-issued driver's licenses and identification documents.

While much of the implementation is the responsibility of the states, DHS understands it has an important role to play. Since promulgation of the REAL ID regulation, DHS has worked closely with states to help improve both their licenses and licensing processes. Since 2008, DHS has awarded over \$183 million in grants to states to assist with improvements to facility infrastructure, information technology systems, physical security features of identity documents, business practices, and equipment purchases. These enhancements have enabled states—including states with laws against compliance with the Act—to make significant progress toward achieving compliance with many or most REAL ID requirements. Additionally, the Administration strongly supported the PASS ID Act legislation in the last Congress, which would have comprehensively addressed challenges with REAL ID implementation identified by the states.

Notwithstanding the tremendous progress being made to meet the REAL ID requirements, states have indicated they will need more time to comply. Therefore, DHS exercised its authority to establish a new compliance deadline of January 15, 2013. The Department expects that states will continue to make progress, and we will continue to work closely with governors, state legislators, state homeland security advisors, and department of motor vehicle leadership to assist in efforts to meet the requirements of the Act.

The Honorable Peter T. King  
Page 2

Thank you again for your letter. I appreciate your support of the Department's efforts to prevent terrorism and improve the reliability of personal identification documents through REAL ID. Chairmen Sensenbrenner and Smith, who co-signed your letter, will receive separate, identical responses. Should wish to discuss this further, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock", with a stylized flourish at the end.

Nelson Peacock  
Assistant Secretary  
Office of Legislative Affairs

**MAY 11 2011**

*Assistant Secretary for Legislative Affairs*

**U.S. Department of Homeland Security**  
Washington, DC 20528



**Homeland  
Security**

The Honorable Candice S. Miller  
Chairman  
Subcommittee on Border  
and Maritime Security  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman Miller:

Thank you for your recent letter regarding the appearance of Department of Homeland Security (DHS) witnesses before Congress and your Subcommittee on Border and Maritime Security. I appreciate the opportunity to respond to the concerns raised in your letter.

DHS supports meaningful Congressional oversight. In the 111<sup>th</sup> Congress, a total of 423 DHS witnesses testified in 304 hearings. This imposed a significant time burden on DHS witnesses and members of Congress alike, and I share your desire to streamline the hearing process. For hearings to provide the maximum value for Congress, I believe our witnesses must be able to engage in frank and candid conversation with the Committee. The time-honored tradition of placing federal witnesses on separate panels promotes the free exchange of ideas and it should remain the standard under which DHS witnesses appear before Congress.

The routine placement of federal government personnel on the same panel as private witnesses does not enhance the efficiency of hearings or the quality of testimony. This practice may introduce private, legal, commercial, or other interests that can compromise the government's position and distract from a clear presentation of the Department's views. In the hearings referenced in your letter, only eight of them included a DHS witness testifying with private sector witnesses—fewer than 3 percent of the time. Certainly, there are circumstances where a DHS witness may share a panel; however, this should continue to be the exception not the rule.

I appreciate the demands that the Congressional schedule places on Members, and I have instructed our Office of Legislative Affairs to accommodate the Committee to the extent possible while ensuring that our witnesses have adequate time to prepare testimony and appear before the Committee. I look forward to

continuing to work with you and the Committee Members to ensure that DHS witnesses appear before the Committee in support of your oversight responsibilities and our mutual goal to secure America. Please do not hesitate to contact me at (202) 447-5890 with any further suggestions about ways to continue improving DHS's relationship with Congress.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock", with a stylized, flowing script.

Nelson Peacock  
Assistant Secretary  
Office of Legislative Affairs



Secretary

U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

September 6, 2011

The Honorable Patrick Meehan  
Chairman  
Subcommittee on Counterterrorism and Intelligence  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Representative Meehan:

Thank you for your letter regarding the Department of Homeland Security's role in the analysis, distribution, and response to the cache of information that was collected from Usama Bin Ladin's compound during the successful special forces operation. I have enclosed a paper that provides responses to your specific questions about DHS's involvement.

DHS has worked with our counterterrorism partners throughout the Intelligence Community to keep our homeland security partners informed and ensure that timely, appropriate information is provided to stakeholders. I agree that it is essential that DHS leverage this victory to help keep our stakeholders informed of the current threat. The enclosure details efforts to date.

Thank you again for your letter. I look forward to continuing to work with you on this and other homeland security matters. If I can be of any further assistance please do not hesitate to contact me on (202) 282-(b)(6)

Yours very truly,

A handwritten signature in black ink, appearing to read "Janet Napolitano", with a long horizontal stroke extending to the right.

Janet Napolitano

Enclosure

Secretary

U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

September 6, 2011

The Honorable Patrick Meehan  
Chairman  
Subcommittee on Counterterrorism and Intelligence  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Representative Meehan:

Thank you for your letter regarding the Department of Homeland Security's role in the analysis, distribution, and response to the cache of information that was collected from Usama Bin Ladin's compound during the successful special forces operation. I have enclosed a paper that provides responses to your specific questions about DHS's involvement.

DHS has worked with our counterterrorism partners throughout the Intelligence Community to keep our homeland security partners informed and ensure that timely, appropriate information is provided to stakeholders. I agree that it is essential that DHS leverage this victory to help keep our stakeholders informed of the current threat. The enclosure details efforts to date.

Thank you again for your letter. I look forward to continuing to work with you on this and other homeland security matters. If I can be of any further assistance please do not hesitate to contact me on (202) 282-(b)(6)

Yours very truly,

A handwritten signature in black ink, appearing to read "Janet Napolitano", with a long horizontal flourish extending to the right.

Janet Napolitano

Enclosure



**Homeland  
Security**

SEP 12 2011

The Honorable Peter T. King  
Chairman  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman King:

Thank you for your letter regarding the Department of Homeland Security (DHS) Headquarters Consolidation Project. The Department sincerely appreciates your leadership and the Committee's support for this important initiative to enhance DHS mission effectiveness.

Based on the levels in the Fiscal Year 2011 Continuing Resolution, the Department is working with the General Services Administration to update the long-term strategy for Headquarters consolidation, both on and off the St. Elizabeths campus. As you know, neither the Department nor GSA was adequately funded in Fiscal Year 2011 to keep the St. Elizabeths project on the original schedule. Additionally, the President has directed the Department to continue to reduce real estate costs to support the \$3 billion saving target across the Federal Government. In order to contribute to this savings goal, the Department is currently looking at ways to better utilize existing space while reducing costs.

Funding levels in the Administration's Fiscal Year 2012 budget request for both DHS and GSA would have enabled the Department to complete the phase one facilities and to continue work on the consolidation of the Department's operations centers, the most vital aspect of the St. Elizabeths effort. However, the Senate's markup of the appropriations bill reduces funding for St. Elizabeths by \$100 million while the FY 2012 House passed bill eliminates funding for the project in FY 2012, further impacting the planned construction and consolidation.

While the current fiscal environment offers an opportunity to re-assess the overall Headquarters consolidation strategy to further minimize costs, the Department remains committed to the goals of the DHS Headquarters Consolidation Project in order to increase operational effectiveness and efficiencies.

DHS welcomes your interest in this important matter and looks forward to working with you on this and future homeland security issues. Should you wish additional assistance, please contact me at (202) 447-5890.

Respectfully,

A handwritten signature in blue ink, appearing to read "Rafael Borrás".

Rafael Borrás  
Under Secretary for Management



**OCT 19 2011**



**Homeland  
Security**

The Honorable Patrick Meehan  
Chairman  
Subcommittee on Counterterrorism and Intelligence  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman Meehan:

Thank you for your August 24, 2011 letter requesting information on the Department of Homeland Security's (DHS) role in screening Iraqi refugee applicants, and how that process has evolved to address security concerns.

DHS is continually working with interagency stakeholders to improve and expand procedures for vetting prospective immigrants, asylum seekers, refugees, and visa applicants. The interagency vetting processes in place today are more robust and consider a far broader range of information than in previous years. We share in your commitment to ensure the prevention of terrorists exploiting the refugee resettlement program by employing the most rigorous screening regime possible.

With the advent of large-scale processing of Iraqi refugees in May 2007, DHS implemented an Administration-coordinated, enhanced background and security check process for Iraqi refugees applying for resettlement in the United States. For example, the fingerprints of refugee applicants are checked against biometric holdings in the Department of Defense and Federal Bureau of Investigation systems, as well as DHS's Automated Biometric Identification System. The security check regime, including both biographic and biometric checks, has been enhanced over the last several years as new opportunities and interagency partnerships with law enforcement and intelligence communities have been identified.

To further bolster security checks, DHS has worked closely with its intelligence and law enforcement counterparts to develop new mechanisms that identify high-risk applicants based on a broader set of data, including information that is not otherwise available to DHS or the Department of State for vetting purposes. As new checks are developed and systems mature, DHS routinely screens previously admitted refugees against this data and provides derogatory information to appropriate law enforcement agencies. These enhancements are a reflection of DHS's commitment to conduct the most thorough checks possible to prevent dangerous individuals from gaining access to the United States through the refugee program.

The latest enhancement to the refugee security check regime involves a new "pre-departure" check shortly before refugees are scheduled to travel to the United States. It is intended to identify whether any new derogatory information exists since the initial checks were conducted. These pre-departure checks went into effect in late 2010, and no case is approved until results from all security checks have been received and analyzed.

The admission of refugees into the United States is a long-standing American tradition and reflects our highest values and aspirations to protect the vulnerable and provide a safe haven for the persecuted. Moreover, many Iraqi refugees have been targeted for persecution precisely because of their work with and support for the American mission in Iraq. The Administration does not believe that we should abandon individuals who have worked and fought with us side by side.

The Department provided a classified briefing for the House Committee on Homeland Security staff on May 18, 2011 on this topic. We would be happy to provide an update to that briefing with more detailed responses to your questions in a classified setting.

Thank you again for your letter. Should you need additional assistance, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock", with a stylized, flowing script.

Nelson Peacock  
Assistant Secretary  
Office of Legislative Affairs

cc: The Honorable Hillary Clinton, Secretary of State

**NOV 03 2011**



**Homeland  
Security**

The Honorable Michael T. McCaul  
Chairman  
Subcommittee on Oversight,  
Investigations and Management  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your September 14, 2011 letter concerning the locations and responsibilities of Department of Homeland Security (DHS) personnel outside the United States.

DHS deploys personnel abroad to strengthen homeland security. Our personnel work cooperatively with international partners to identify, prevent, deter, investigate, and disrupt threats, and manage homeland security risks through information and knowledge sharing and cooperation in joint operations. Direct cooperation with foreign officials enhances collaboration and strengthens aviation security, maritime security, and global supply chain security. Working abroad, our personnel pursue enhanced international collaboration in technology development and evaluation, and they develop norms, standards, and regulatory environments. By providing capacity building, training, and technical assistance in partnership with the Departments of State and Defense, DHS personnel abroad protect the homeland by strengthening weak links in the global systems that move people and goods.

DHS personnel are present in more than 70 countries worldwide, with 1,548 personnel assigned permanently and approximately 80 personnel assigned on temporary duty for more than 60 days to locations outside of the United States. Secretary Napolitano is currently reviewing the DHS international presence abroad to ensure alignment with DHS international priorities and strategies. Most DHS personnel abroad are funded directly by appropriations, or in some cases by immigration benefit fees or other means.

To answer your questions in more detail, I have enclosed a document that describes the number, locations, and responsibilities of DHS personnel abroad.

The Honorable Michael McCaul  
Page 2

Thank you again for your letter. Should you need additional assistance, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock", with a stylized flourish at the end.

Nelson Peacock  
Assistant Secretary  
Office of Legislative Affairs

Enclosure

**ENCLOSURE IN RESPONSE TO REP. MCCAUL'S SEPTEMBER 14, 2011 LETTER**

**Permanently Assigned Personnel Abroad**

The Department of Homeland Security currently has 1,548 personnel permanently assigned to locations outside the United States. Table 1 provides the number of these personnel from each DHS Component:

<b>Table 1: Breakdown of Permanent Personnel Assigned Outside the U.S. By Component</b>	
<b>Component</b>	<b>Number of Personnel Permanently Assigned Outside U.S.</b>
U.S. Customs and Border Protection	643
U.S. Coast Guard	384
U.S. Immigration and Customs Enforcement	279
U.S. Secret Service	93
U.S. Citizenship and Immigration Service	79
Transportation Security Administration	58
Office of International Affairs (DHS HQ)	5
Federal Law Enforcement Training Center	2
Federal Emergency Management Agency	2
National Protection & Programs Directorate	2
Science and Technology Directorate	1
<b>Total</b>	<b>1,548</b>

**Places where DHS has permanently assigned personnel are shown below:**

Afghanistan	Costa Rica	Hong Kong	Mexico	Spain
Argentina	Cuba	India	Morocco	Sri Lanka
Aruba	Denmark	Indonesia	Netherlands	Sweden
Australia	Dominican Republic	Iraq	Netherlands	Switzerland
Austria	Ecuador	Ireland	Antilles	Taiwan
Bahamas	Egypt	Israel	Oman	Thailand
Bahrain	El Salvador	Italy	Pakistan	Trinidad and Tobago
Barbados	Estonia	Jamaica	Panama	United Arab Emirates
Belgium	France	Japan	Peru	United Kingdom
Bermuda	Georgia	Jordan	Philippines	Venezuela
Botswana	Germany	Kenya	Poland	Vietnam
Brazil	Ghana	Korca, Republic of	Portugal	Yemen
Bulgaria	Greece	Kuwait	Romania	
Cambodia	Guatemala	Liberia	Russia	
Canada	Haiti	Malaysia	Saudi Arabia	
China	Honduras	Malta	Singapore	
Colombia			South Africa	



## **DHS TDY Personnel Abroad**

DHS has approximately 80 personnel assigned on temporary duty (TDY) for more than 60 days to locations outside the United States.

## **Functions of DHS Personnel Assigned Abroad**

Personnel from DHS Components perform the following functions outside the United States:

**U.S. Customs and Border Protection (CBP):** CBP works globally to prevent, identify and interdict the intended entry of people or goods that would violate U.S. law or interests. CBP maintains extensive operational, liaison and technical relationships to accomplish this goal, including the Immigration Advisory Program, Preclearance Operations, the Container Security Initiative, International Expedited Traveler Programs, the Customs-Trade Partnership Against Terrorism, International Border Enforcement Teams and other programs. Further, CBP maintains international partnerships and relationships that enable it to share its best practices with foreign governments. It provides training and technical assistance to foreign governments and establishes international policies through organizations such as the World Customs Organization (WCO), International Civil Aviation Organization (ICAO), and other multilateral standards bodies.

**Federal Emergency Management Agency (FEMA):** FEMA engages internationally to add value to its domestic mission through the exchange of knowledge with foreign partners to evaluate best practices, procedures, and policies that may enhance those of the United States. FEMA also supports U.S. geopolitical and operational priorities through, for example, the management of the North Atlantic Treaty Organization's Senior Civil Emergency Planning Committee.

**Federal Law Enforcement Training Center (FLETC):** FLETC participates in the International Law Enforcement Academies and other international training programs.

**U.S. Immigration and Customs Enforcement (ICE):** ICE protects our borders by conducting multi-faceted, international law enforcement operations and partnering with foreign and domestic counterparts to combat criminal organizations and prevent terrorist activities. In addition to its investigative work, ICE's international activities support its removal operations and U.S. visa adjudications through the Visa Security Program. Through work with the WCO, Interpol, Virtual Global Task Force, Financial Action Task Force, and other multilateral bodies, ICE builds global consensus and standards.

**National Protection & Programs Directorate (NPPD):** NPPD partners with global stakeholders in the areas of: understanding and assessing risk; critical infrastructure protection; cybersecurity and communications; biometric identity verification services; and securing and protecting federal facilities. Through global partnerships, NPPD enhances the safety, protection, and resilience of the United States and its allies. US-VISIT provides specific technical assistance in building biometric identity screening capabilities for border security and immigration management to the United Kingdom and Australia.



**Office of International Affairs:** DHS attachés and liaison officers selected by and under the direction and leadership of the Office of International Affairs plan, coordinate, manage, lead, and execute DHS policies and strategies and activities in critical foreign countries.

**Science & Technology Directorate (S&T):** S&T partners with foreign governments and institutions with a proven record of scientific excellence to learn from foreign research and share knowledge about U.S. standards to support the evolution of compatible approaches.

**Transportation Security Administration (TSA):** TSA works with ICAO and appropriate aeronautic authorities of foreign governments to address security concerns on passenger flights by foreign air carriers in foreign air transportation. To this end, TSA engages globally to improve the foundation of sound security worldwide through compliance enforcement, outreach/engagement, and capacity development. TSA also deploys Federal Air Marshals globally to protect U.S. flagged air carriers and assumes a leadership role in ICAO and other bodies dedicated to transportation security.

**U.S. Citizenship and Immigration Services (USCIS):** USCIS engages internationally to extend humanitarian protection and assistance and to provide other immigrant benefits and services, while protecting national security and combating fraud. USCIS also provides subject matter expertise to foreign governments, international organizations and other federal agencies on immigration. USCIS Refugee Officers are routinely overseas conducting refugee admission interviews but are typically on rotations of less than 60 days.

**United States Secret Service (USSS):** USSS works internationally to safeguard the nation's financial infrastructure, payment systems and preserve the integrity of the nation's economy. The Secret Service has jurisdiction to investigate all forms of financial crimes including computer fraud, credit card fraud, the counterfeiting of US currency, identity theft, bank fraud, and money laundering. In addition, the Secret Service protects the President, Vice President, and other U.S. Government officials while they travel overseas, and routinely engages in effective partnerships with international partner organizations when foreign heads of state/heads of government travel to the United States.

**United States Coast Guard (USCG):** USCG establishes, improves, sustains, and leverages international cooperation and partnerships to create, promote, and ensure a transparent, safe, secure and environmentally sound maritime domain in support of USCG missions and national interests. USCG international engagement consists of activities that enable and strengthen international maritime authorities, build international competencies and capabilities, and develop international partnerships that advance U.S. Government and Coast Guard missions and interests around the world. With those nations with whom we share a maritime boundary, the USCG seeks to leverage partnerships as a force multiplier. With others, the USCG contributes to the development of and enforces compliance with international standards and shares knowledge and capability, including through a series of regional fora and the International Maritime Organization. The USCG further supports war fighting as a member of the U.S. Armed Forces.

**Funding for DHS Personnel Abroad**

DHS personnel serving abroad are funded directly by Component appropriations or immigration benefit fees in most cases, with a small number of positions funded by the Department of State, the Department of Defense, and other sources.



**Homeland  
Security**

**NOV 23 2011**

The Honorable Peter T. King  
Chairman  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your recent letter to Secretary Napolitano and Attorney General Eric Holder requesting that the Department of Homeland Security (DHS) and the Department of Justice not seek to remove Daoud Chehazeh without first questioning him under oath about what role he, Anwar Awlaki, and Eyad al-Rababah played in the September 11, 2001 terrorist attacks.

Although DHS is involved in litigation that may lead to Mr. Chehazeh's eventual removal from the United States, his removal is not imminent. Mr. Chehazeh is not subject to a final order of removal and is not in DHS custody.

Additionally, DHS is ready and willing to assist the Federal Bureau of Investigation (FBI) the lead investigative agency in counterterrorism matters—in any interview of Mr. Chehazeh, should the FBI decide to question him under oath.

Thank you again for your letter. Should you wish to discuss this matter further, do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock".

Nelson Peacock  
Assistant Secretary  
Office of Legislative Affairs

cc: Ronald Wiech, Assistant Attorney General  
Department of Justice, Office of Legislative Affairs

JAN 27 2012

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



**Homeland  
Security**

The Honorable Michael T. McCaul  
Chairman  
Subcommittee on Oversight, Investigations,  
and Management  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Mr. Chairman:

I write in response to your letter regarding how Department of Homeland Security (DHS) Components used funds provided from the Treasury Asset Forfeiture Fund.

Each year, DHS Components receive funds from the Treasury Asset Forfeiture Fund to support law enforcement activities. Enclosed is a description of the activities supported by these funds within each DHS Component. DHS Components receive two types of funds: Super Surplus funds and mandatory funds. Pursuant to Section 536 of the Fiscal Year 2010 *Department of Homeland Security Appropriations Act* (P.L. 111-83), funds identified for transfer from the Super Surplus Fund may not be obligated until approval is provided by the Appropriations Committee. Mandatory funds are distributed under the authority provided in enabling legislation for the *Treasury Forfeiture Fund Act* (31 USC § 9703) and do not require prior approval from the Appropriations Committee.

Should you have any questions, please contact me or Jeffrey Readinger at (202) 447-5890.

Sincerely,

A handwritten signature in black ink, appearing to read "Nelson Peacock", with a stylized flourish at the end.

Nelson Peacock  
Assistant Secretary for Legislative Affairs

Enclosure

<b><u>U.S. CBP</u></b>		<b>2010</b>
	Mandatory Expenses	\$35.753
	Super Surplus	<u>\$29.590</u>
	<b>CBP Total Approved Financial Plan</b>	<b>\$65.343</b>
<b><u>U.S. ICE</u></b>		
	Mandatory Expenses	\$132.709
	Super Surplus	<u>\$21.431</u>
	<b>ICE Total Approved Financial Plan</b>	<b>\$154.140</b>
<b><u>U.S. SECRET SERVICE</u></b>		
	Mandatory Expenses	\$103.662
	Super Surplus	<u>\$18.062</u>
		<b>\$121.724</b>
<b><u>U.S. COAST GUARD</u></b>		
	Mandatory Expenses	\$1.094
	Super Surplus	<u>\$3.086</u>
	<b>US Coast Guard Total Approved Financial Plan</b>	<b>\$4.180</b>
<b><u>FLETC</u></b>		
	Mandatory Expenses	\$0.000
	Super Surplus	<u>\$0.345</u>
	<b>FLETC Total Approved Financial Plan</b>	<b>\$0.345</b>
<b><u>Total TEOAF Expenditures For DHS Agencies</u></b>		<b><u>\$345.732</u></b>

**U.S. CUSTOMS AND BORDER PROTECTION -- FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt. (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
<b>MANDATORY EXPENSES:</b>					
A. Seizure Investigative Costs & Asset Management					
• Salaries					
• Salaries - Existing Positions	\$13.700	\$13.700	\$15.000	\$15.000	Funding is requested for 15 positions within the National Finance Center (NFC), 11 positions within the Seized and Forfeited Property Division (SFPD), 130 Seized Property Custodians within OFO, 9 positions within OFO Headquarters, and 4 positions within OBP
• Salaries - New Positions	\$0.000	\$0.000	\$0.000	\$0.000	These funds are requested to support 50 OBP positions (\$3.707), 43 OFO positions, and 1 OTD position
• Seized Property Oversight Travel	\$0.283	\$0.154	\$0.200	\$0.200	Funds are used to conduct unannounced office and seized property vault inspections.
• Overtime	\$0.450	\$0.450	\$0.610	\$0.580	Funds support overtime worked by Seized Property Custodians & Specialists involved in securing seized merchandise and conducting Border Patrol security operations for narcotics destruction.
					<b>INCREASE: \$160 (Approved 7/23/10)</b>
• Supplies	\$0.370	\$0.235	\$0.365	\$0.340	Funds are for supplies and equipment, and aircraft and vessel items directly related to support the handling and storage of seized property and narcotics.
					<b>MID-YEAR INCREASE: \$165 to fix the flood damages to Del Rio vault. (Approved 6/15/10)</b>
• Advertisement	\$1.480	\$1.187	\$1.150	\$1.123	Funds defray escalating costs for posting seizures subject to forfeiture as required by regulations and mandated by court decrees. Also ensures perfection of forfeiture on legacy Border Patrol/INS seizure cases initiated under Title 8 and subject to CAFRA requirements.
					<b>REPROGRAMMED \$0.050 from Category J. Seized Property Training (Approved 5/13/10)</b>
					<b>MID-YEAR: REPROGRAMMED \$0.067 from Category A. Seized &amp; Forfeited Property Division (Approved 6/15/10)</b>
					<b>MID-YEAR: REPROGRAMMED \$0.033 from Category A. Accounting Services (Approved 6/15/10)</b>
• Storage	\$0.000	\$0.000	\$0.000	\$0.000	These funds are requested to pay expenses related to the storage and securing of seized property and narcotics. Expenses include vault alarm services, upgrades of temporary storage facilities, routine facility maintenance and repair, locksmithing, and videotapes and cameras for CCTV systems.



**U.S. CUSTOMS AND BORDER PROTECTION – FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt. (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
• GSA Rent	\$0.000	\$0.000	\$0.000	\$0.000	Request funds to pay GSA for leased space associated with seized property operations.
• Accounting Services	\$0.100	\$0.100	\$0.067	\$0.067	Funds to pay NFC (previously ASD) overtime, travel, supplies, training and equipment expenses.  <b>MID-YEAR: REPROGRAMMED \$.033 to Category A. Advertising (Approved 6/15/10)</b>
• Seized & Forfeited Property Division	\$0.350	\$0.200	\$0.133	\$0.133	Funds are requested for SFPD's travel, supplies, overtime, contractors, training, and equipment.  <b>MID-YEAR: REPROGRAMMED \$.067 to Category A. Advertising (Approved 6/1/10)</b>
<b>Subtotal, Seizure Investigative Costs &amp; Asset Management</b>	<b>\$16.733</b>	<b>\$16.026</b>	<b>\$17.525</b>	<b>\$17.443</b>	
<b>B. Contract Services</b>					
• Vehicle Consignment & Disposal Contract	\$13.430	\$10.150	\$10.000	\$10.000	Funds are requested to support costs associated with the contract.
• Medical Services	\$0.000	\$0.000	\$0.000	\$0.000	Funds are requested for costs associated with medical services in support of seized narcotics.
<b>Subtotal, Contract Services</b>	<b>\$13.430</b>	<b>\$10.150</b>	<b>\$10.000</b>	<b>\$10.000</b>	
<b>C. Awards to Informers</b>	<b>\$0.000</b>	<b>\$0.000</b>	<b>\$0.000</b>	<b>\$0.000</b>	These funds will compensate informers under section 619 of the Tariff Act of 1930 (19 U.S.C. 1619).
<b>D. Payment of Liens</b>	<b>\$0.603</b>	<b>\$0.477</b>	<b>\$0.300</b>	<b>\$0.092</b>	To fund qualified third-party interests in accordance with Treasury guidelines on seized and forfeited property.
<b>E. Payment for Remission &amp; Mitigation</b>	<b>\$2.094</b>	<b>\$1.398</b>	<b>\$3.109</b>	<b>\$3.084</b>	Funding is requested for anticipated expenditures related to the return of partial mitigation of properties seized by CBP.  <b>MID-YEAR DECREASE: \$1.000 (Approved 5/4/10)</b>  <b>INCREASE: \$.589 (Approved 9/23/10)</b>  <b>REPROGRAM FROM ICE REMISSIONS: \$.020 (Approved 9/28/10)</b>
<b>F. Claims of Parties in Interest</b>	<b>\$0.000</b>	<b>\$0.000</b>	<b>\$0.000</b>	<b>\$0.000</b>	These funds are for payment of claims of parties in interest to property disposed of under the Tariff Act of 1930 (19 U.S.C. 612(b)).
<b>G. Equitable Sharing Payments</b>	<b>\$0.179</b>	<b>\$0.258</b>	<b>\$0.300</b>	<b>\$0.016</b>	Funding is requested for equitable sharing of forfeiture proceeds with state and local law enforcement agencies that have assisted in seizing assets.  <b>MID-YEAR DECREASE: \$.200 (Approved 5/4/10)</b>



**U.S. CUSTOMS AND BORDER PROTECTION – FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt. (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
I. Reimburse State & Locals - Joint Operations	\$0.085	\$0.425	\$0.300	\$0.240	Funding is requested to reimburse state and local law enforcement agencies for overtime costs incurred while supporting joint special operations initiated by local CBP offices.  <b>MID-YEAR: REPROGRAMMED \$.200 to Category J. Narcotics Destruction (Approved 6/15/10)</b>
J. Data Systems, Training, Contracting for Services					
• Forfeiture Support Associates (FSA)	\$0.000	\$0.451	\$0.500	\$0.500	OBP requests continued funding of the rider contract with FSA, which is managed by DOJ, for support services. FSA personnel perform duties that would otherwise be performed by civilian full time employees (FTE) or by detailed Border Patrol Agents.
• National Automotive Dealers Assoc. (NADA)	\$0.000	\$0.000	\$0.000	\$0.000	This request will provide online NADA book guides for all types of vehicles. This will ensure that personnel utilize the most accurate appraisal when placing an estimated value on motor vehicles and obtain a one-year license for unlimited access to NADA data.
• Seized Property Training (non-OIT)	\$0.387	\$0.428	\$0.300	\$0.300	These funds will provide non-OIT training as well as one FP&F National Conference and one SFPD National Conference.  <b>REPROGRAMMED \$.100 to Category J. Narcotics Destruction (Approved 5/13/10)</b>  <b>REPROGRAMMED \$.050 to Category A. Advertising (Approved 5/13/10)</b>
• Narcotics Destruction	\$0.900	\$1.265	\$1.600	\$1.578	Funding is requested to transport and destroy high-risk property line items including controlled substances and other contraband and travel for officers subpoenaed in cases involving same.  <b>REPROGRAMMED: \$.100 from Category J. Seized Property Training (Approved 5/13/10)</b>  <b>REPROGRAMMED: \$.200 from Category I. Reimburse State &amp; Locals - Joint Operations (Approved 6/15/10)</b>  <b>MID-YEAR INCREASE \$.300 (Approved 6/15/10)</b>
• SEACATS	\$2.000	\$1.900	\$2.500	\$2.500	Funds are requested to support existing and additional functionality currently being deployed.
• Freon Destruction	\$1.200	\$0.000	\$0.000	\$0.000	Funding is requested to transport and destroy freon.
<b>Subtotal Data Systems, Training, Contracting for Services</b>	<b>\$4.487</b>	<b>\$4.044</b>	<b>\$4.900</b>	<b>\$4.878</b>	
<b>SUBTOTAL (MANDATORY)</b>	<b>\$37.611</b>	<b>\$32.778</b>	<b>\$36.434</b>	<b>\$35.753</b>	

**U.S. CUSTOMS AND BORDER PROTECTION – FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt. (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
<b><u>SUPER SURPLUS EXPENSES:</u></b>					
• Special Purpose Off-road Vehicles and Related Equipment	\$0.000	\$0.500	\$1.000	\$1.000	Funding is for various types of off-road vehicles (ATV's, snowmobiles, jet skis, and mountain bikes) and related equipment for use in the many remote and/or rough terrain locations in which CBP operates.
• Specialty Equipment for Intel. Officers	\$0.000	\$0.600	\$0.250	\$0.250	Funding is to purchase specialized equipment for Intelligence Agents, such as cell phone data extractors, mapping and IT equipment, and GPS tracking devices. The addition of this equipment will enhance the capacity and efficiency of agents gathering intelligence on smuggling organizations that affect National Security.
• Specialty Equipment Field – Field Detection	\$0.000	\$0.000	\$2.500	\$2.500	Funding is for specialized field detection equipment.
• Specialty Officer Safety Equipment	\$0.000	\$1.000	\$0.250	\$0.250	Funding is for specialized officer safety equipment, such as helmets, flashlights, and hydration gear.
• Incinerators	\$0.000	\$0.000	\$4.000	\$0.000	Funding is for the purchase of two additional incinerators, one for (b)(7)(E) and one for (b)(7)(E).
• Narcotics Destruction Security Detail	\$0.000	\$0.000	\$0.640	\$0.540	Funding is for CBP to assume from ICE the responsibility for providing security for seized narcotic property destructions.
• Imaging Machines	\$0.000	\$0.000	\$6.800	\$6.800	Funding is for the purchase and installation of Non-Intrusive Inspection (NII) equipment.
• Vaults	\$4.800	\$1.500	\$3.400	\$3.250	Funding is for major vault construction to facilitate the safeguarding of seized and forfeited property in the following locations: (b)(7)(E) (b)(7)(E)
• CBP - Southwest Border Initiative	\$0.000	\$0.000	\$15.000	\$15.000	Funds will support the construction of Border Patrol facilities in Southwest Border locations (Animas Valley, NM, and Nogales, AZ) and the purchase of necessary equipment for these facilities. The construction of these facilities is critical for the Administration's Southwest Border enforcement effort, as the existing facilities are insufficient for Border Patrol needs, and would not accommodate the upcoming deployment of an additional 1,000 new Border Patrol agents. (Approved 7/22/10)
<b>SUBTOTAL (SUPER SURPLUS)</b>	<b>\$4.800</b>	<b>\$3.600</b>	<b>\$33.840</b>	<b>\$29.690</b>	
<b>TOTAL CBP</b>	<b>\$42.411</b>	<b>\$36.378</b>	<b>\$70.274</b>	<b>\$65.343</b>	



**U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT – FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
<b>MANDATORY EXPENSES:</b>					
<b>A. Seizure Investigative Costs &amp; Asset Management</b>					
• POI/POE	\$8.499	\$9.600	\$9.602	\$9.594	Funding is requested to reimburse OI for the purchase of information and evidence associated with specific seizures.  <b>REPROGRAMMED \$140 from Category A. Other Investigative Costs (Approved 6/29/10)</b>  <b>REPROGRAMMED \$300 from Category J. Asset Identification and Removal Groups (Approved 8/10/10)</b>  <b>REPROGRAMMED \$161,948 from Category A. Other Investigative Costs (Approved 8/30/10)</b>
• Other Investigative Costs	\$9.500	\$3.389	\$3.198	\$3.197	Funds are for seizure-related investigative costs other than POI/POE. A portion of these costs will be attributed to additional travel required to examine seized property at the 3 COFS under the new general property contract.  <b>REPROGRAMMED \$140 to Category A. POI/POE (Approved 6/29/10)</b> <b>REPROGRAMMED \$161,948 to Category A. POI/POE (Approved 8/30/10)</b>
• Salaries					
• Salaries - Existing Positions	\$5.900	\$5.612	\$7.400	\$7.400	Funding will be used to cover existing positions in the Office of Investigations supporting the asset forfeiture program, both at the Headquarters and in the field offices.
• Seized Property Oversight Travel	\$0.035	\$0.031	\$0.050	\$0.033	Funds are for unannounced office and seized property vault inspections, as well as oversight visits of the national seized property contractor.
<b>Subtotal, Seizure Investigative Costs &amp; Asset Management</b>	<b>\$23.934</b>	<b>\$18.632</b>	<b>\$20.250</b>	<b>\$20.224</b>	
<b>C. Awards to Informers</b>	\$0.000	\$0.000	\$0.200	\$0.186	These funds will compensate informers under section 619 of the Tariff Act of 1930 (19 U.S.C. 1619).  <b>MID-YEAR INCREASE: \$100 (Approved 5/4/10)</b>
<b>D. Payment of Liens &amp; Mortgages</b>	\$2.990	\$1.916	\$4.000	\$1.872	To fund qualified third-party interests in accordance with Treasury guidelines on seized and forfeited property.  <b>MID-YEAR: \$1,000 REPROGRAMMED FROM IRS CATEGORY D: LIENS &amp; MORTGAGES (Approved 5/4/10)</b>

**U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT -- FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
E. Payment for Remission & Mitigation	\$115.631	\$24.569	\$12.980	\$8.150	<p>The funds are reserved for anticipated expenditures related to the return or partial mitigation of properties seized by ICE.</p> <p><b>MID-YEAR DECREASE: \$2.000 (Approved 5/4/10)</b></p> <p><b>REPROGRAM TO CBP REMISSIONS \$0.020 (Approved 9/28/10)</b></p>
G. Equitable Sharing Payments	\$66.032	\$94.820	\$90.000	\$82.535	<p>This provides equitable sharing payments to foreign countries, other federal, state and local law enforcement agencies participating in ICE seizure investigations. ICE pays equitable sharing on both ICE and CBP forfeitures.</p> <p><b>MID-YEAR DECREASE: \$20.000 (Approved 5/4/10)</b></p> <p><b>INCREASE: \$20.000 (Approved 8/3/10)</b></p>
H. Services of Experts and Consultants	\$0.000	\$0.025	\$0.025	\$0.000	<p>Funds to be used to pay for the services of a consultant or expert to provide advice on the management, preservation and liquidation of a variety of investments that were seized or forfeited as a result of ICE investigations.</p>
I. Reimburse State & Local - Joint Operations	\$6.209	\$7.695	\$7.307	\$7.292	<p>Funds are to reimburse state and local law enforcement offices for overtime costs incurred while supporting joint special operations initiated by local ICE offices.</p> <p><b>REPROGRAMMED \$0.050 from IRS Category I. Reimburse State &amp; Local - Joint Operations (Approved 7/12/10)</b></p> <p><b>REPROGRAMMED \$0.045 from Category J. Evidence/Narcotics Destruction (Approved 7/12/10)</b></p> <p><b>REPROGRAMMED \$0.200 from Category J. Asset Identification and Removal Groups (Approved 8/10/10)</b></p> <p><b>INCREASE: \$0.012 (Approved 9/30/10)</b></p>
J. Data Systems, Training, Contracting for Services					
• Treasury Computer Forensics Program (formerly CFS)	\$4.319	\$3.010	\$1.726	\$1.706	<p>The requested funding will support the USICE portion of the joint ICE/IRS-CI/USSS Computer Forensic Program development and training.</p> <p><b>INCREASE BY \$24K (Approved 3/4/10)</b> <b>Transferred from IRS</b></p>
• Asset Identification and Removal Group (AIRG)	\$9.487	\$10.488	\$10.200	\$9.880	<p>To cover expenses incurred for contract services utilized in the AIRG program nationwide, to include a refresh of IT equipment used exclusively by ICE AIRG personnel.</p> <p><b>REPROGRAMMED \$0.500 to Category I. Reimburse State &amp; Local - Joint Operations (\$0.200) and Category A. PO/POE (\$0.300) (Approved 8/10/10)</b></p>

**U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT – FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
• Training & Travel	\$0.818	\$0.469	\$0.700	\$0.700	Funds will be used to provide travel to training and incidental service, as well as equipment and supplies costs relative to training agents. Investigative training in this area centers on seized property and asset forfeiture issues. The majority of these funds support ICE's two-week Asset Forfeiture and Financial Investigations courses. An approximate utilization of these funds is as follows: AFFI; DOJ Component Seminars; TEOAF Seminars; ICE/CBP Joint Training, COTR Training.
• Seized Property/Evidence Inventory Equipment	\$0.073	\$0.191	\$0.200	\$0.155	Funds will be used to purchase supplies, security and support equipment to be utilized by the Office of Investigations and Office of Professional Responsibility in the tracking, handling, storing, cataloging and disposing of seized property/evidence. Supplies include purchase of narcotics testing kits for ICE and CBP.
• Evidence/Narcotic Destruction	\$0.046	\$0.046	\$0.030	\$0.009	Funding is requested to transport and destroy high-risk property line items including controlled substances and other contraband. It is anticipated that the volume of this destruction will increase significantly in FY2008.  <b>REPROGRAMMED \$.045 to Category I. Reimburse State &amp; Local - Joint Operations (Approved 7/12/10)</b>
<i>Subtotal Data Systems, Training, Contracting for Services</i>	<i>\$14.743</i>	<i>\$14.204</i>	<i>\$12.856</i>	<i>\$12.450</i>	
<b>SUBTOTAL (MANDATORY)</b>	<b>\$229.539</b>	<b>\$161.861</b>	<b>\$147.618</b>	<b>\$132.709</b>	

**U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT -- FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
<b><u>SUPER SURPLUS EXPENSES:</u></b>					
• Southwest Border Violence/Smuggling Initiatives/ Border Enforcement Security Taskforce (BEST)	\$0.000	\$0.000	\$2.000	\$1.790	<p>Funding will be used primarily for equipment to support Border Enforcement Security Taskforces (BESTs) on the Southwest Border, including: robotic equipment for discovering and navigating clandestine tunnels along the Mexican border, GPS trackers, binoculars, and other equipment for BEST officers. Additionally, funding will support a training conference for BESTs.</p> <p><i>Border Enforcement Security Taskforces (BESTs) are comprised of federal, state, tribal and foreign law enforcement agencies with a mission to identify disrupt and dismantle organizations that seek to exploit vulnerabilities along the border and threaten the overall safety of the American public. BESTs and other ICE anti-border violence and smuggling initiatives are uniquely positioned to combat all cross border criminal schemes, including: weapons and contraband smuggling, money laundering, bulk cash smuggling as well as human smuggling/trafficking and transnational gang criminal activity.</i></p>
• David Wilhelm OCDETF Strike Force Build-out	\$0.000	\$0.000	\$1.000	\$1.000	<p>Funds will be used to support the co-location of assets. Through the co-location of investigative assets, the OCDETF Strike Force agencies have successfully identified smuggling organizations, their transportation and distribution networks, money laundering methods and related assets.</p> <p><i>The David G. Wilhelm OCDETF Strike Force is comprised of ICE, DEA, FBI, BATFE, IRS, State and Local law enforcement agencies. The goal of the Strike Force is to conduct significant investigations fully identifying and dismantling narcotics trafficking organizations at the RPOT and CPOT level.</i></p>
• Purchase of Aircraft for Covert Operations	\$0.000	\$0.000	\$3.800	\$3.800	<p>Funding is for the purchase of two aircraft for use in covert criminal investigations that will replace two aircraft that have recently been sent to GSA surplus for auction due to maintenance, safety and reliability issues. These aircraft were used to support successful transnational smuggling cases over a number of years.</p> <p>The 'covert' aircraft will help to construct and support undercover profiles, including utilizing them to "service" criminal organizations requiring air transport to further criminal organization's enterprise.</p>
• National Initiative for Illicit Trade Enforcement database	\$0.000	\$0.000	\$2.000	\$2.000	<p>Funds will be used towards development of the National Initiative for Illicit Trade Enforcement (NIITE) database. ICE, in conjunction with Customs and Border Protection (CBP) and the Department of Defense (DOD), is currently working on the NIITE. The NIITE targets and tracks illicit trade networks who utilize commercial transportation and the Internet. The NIITE generates actionable, investigative and interdiction information resulting in the detection and disruption of illicit transnational networks posing national security and public safety concerns.</p>

**U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT – FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
• Foreign Law Enforcement Assistance and Operations	\$1.000	\$1.000	\$1.875	\$1.815	Funding will support various activities involving foreign law enforcement assistance and operations. This includes Foreign Vetted Units consisting of a select core group of foreign officials working closely with ICE to target criminal organizations that pose a security threat or have a nexus to the United States. Such Vetted Units are established in multiple locations, mostly in Central and South America.
• Hands Across the World	\$1.135	\$0.700	\$0.625	\$0.624	Funding will enhance and augment the investigative capabilities at the Attaché offices where Hands Across the World (HAW) operations have resulted in seizures or the creation of other investigative leads.  <i>The Hands Across the World initiative is an expansion of Operation Firewall, an anti-bulk cash smuggling initiative. Hands across the world synchronizes worldwide multi-national interdiction operations through the use of real-time intelligence sharing between source country and destination country, and is designed to disrupt the movement of funds by criminal organizations.</i>
• Major Case Funding	\$1.471	\$1.175	\$1.250	\$1.154	Funds will be utilized to cover the costs of various investigative activities within ICE Office of Investigations. Some of these activities include, but are not limited to, translation, transcription and duplication services for investigations targeting major criminal organizations and systems that exploit America's critical financial systems.
• Title III	\$6.000	\$6.000	\$6.000	\$6.000	Funding will help defray the costs of Title III court-ordered intercepts, which are very expensive, in investigations that result in seizures and forfeitures.
• Guardian Surge Operation	\$0.000	\$0.000	\$0.400	\$0.400	Funds will be used to support agents to assist Guardian Surge.  <i>Operation Guardian (Guardian) combines the expertise of specific areas of ICE, CBP, FDA Office of Criminal Investigations, Consumer Product Safety Commission, the DOJ Computer Crimes &amp; Intellectual Property Section, FBI, the U.S. Postal Inspection Service, and the USDA to target, interdict and investigate the importation of substandard, tainted and dangerous products being imported into the United States. Guardian member agencies have formed a Guardian Headquarters Working Group (WG), which has undertaken the task of identifying specific commodities as well as the specific ports of entry (POEs) identified via analysis of previous importers records, seizures, and prior investigations.</i>
• Cellphone and Mobile Device Forensic Training	\$0.000	\$0.345	\$0.350	\$0.350	Funds will be used to train Computer Forensic Agents (CFAs) in advanced processing of cellular phones using software and hands-on training. Funds will also be used to provide trainees with cell phone analysis devices for use in the field.

**U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT -- FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
• International Organized Crime Intelligence Center -2 Intelligence Analysts	\$0.000	\$0.000	\$1.300	\$1.300	Funds will be used to support the costs of 9 intelligence analyst contractors. These analysts will support the IOC-2 and the Fusion Center
• Universal Forensic Extraction Devices (Project Switchboard)	\$0.000	\$0.000	\$0.200	\$0.199	Funding will be used to equip and train the field offices with ruggedized devices to identify, disrupt and dismantle criminal transnational gang activity.  <i>Project Switchboard is a program designed to use ruggedized Universal Forensic Extraction Devices (UFEDs) to extract forensic quality evidentiary data from cell phones and smart phones which can be used to illuminate connections that otherwise would not be discovered. Common call analysis can be used by HQ to then generate intelligence leads back to the field for exploitation.</i>
• Forensic Document Laboratory	\$0.000	\$0.000	\$1.000	\$0.999	Funding is for equipment and materials needed for the Forensic Document Laboratory to support a variety of investigations under ICE purview.
<b>SUBTOTAL (SUPER SURPLUS)</b>	<b>\$9.606</b>	<b>\$9.220</b>	<b>\$21.800</b>	<b>\$21.431</b>	
<b>TOTAL ICE</b>	<b>\$239.145</b>	<b>\$171.081</b>	<b>\$169.418</b>	<b>\$154.140</b>	



**U.S. SECRET SERVICE – FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
<b><u>MANDATORY EXPENSES:</u></b>					
A. Seizure Investigative Costs & Asset Management					
• POI/POE	\$0.048	\$0.084	\$0.050	\$0.050	Funding is for the purchase of information or evidence (POI/POE) pursuant to 31 U.S.C. 9703(a)(1)(A), as an investigative cost leading to seizure.
• Advertising	\$0.300	\$0.239	\$0.300	\$0.170	Funding is requested to cover advertising costs associated with USSS seizures.
• Administrative Supplies	\$0.000	\$0.000	\$0.050	\$0.050	Funding is for supply costs associated with administering the USSS Asset Forfeiture Program.
• Investigative Costs Leading to Seizure	\$1.000	\$0.799	\$1.250	\$1.242	Funding is requested for case-related or direct investigative costs associated with seizures and forfeitures.
					<b>REPROGRAMMED \$500 from Category E. Payments for Remission &amp; Mitigation (Approved 6/8/10)</b>
• AFS Administrative Personnel	\$0.451	\$0.450	\$0.730	\$0.501	Funding is for Secret Service's administrative staff for support related to the Asset Forfeiture Program.
<b>Subtotal, Seizure Investigative Costs &amp; Asset Management</b>	<b>\$1.799</b>	<b>\$1.572</b>	<b>\$2.380</b>	<b>\$2.013</b>	
D. Payment of Liens & Mortgages	\$0.120	\$0.060	\$0.750	\$0.551	To fund qualified third-party interests in accordance with Treasury guidelines on seized and forfeited property.
					<b>MID-YEAR: \$500 REPROGRAMMED FROM IRS CATEGORY D: LIENS &amp; MORTGAGES (Approved 5/4/10)</b>
E. Payments for Remission & Mitigation	\$9.966	\$15.282	\$95.500	\$94.338	The funds are reserved for anticipated expenditures related to the return or partial mitigation of properties seized by the USSS.
					<b>INCREASE BY \$3M (Approved 3/2/2010)</b>
					<b>REPROGRAMMED \$500 TO Category A. Investigative Costs Leading to Seizure (Approved 6/8/10)</b>
					<b>INCREASE BY \$7M (Approved 8/24/10)</b>
G. Equitable Sharing Payments	\$2.555	\$5.568	\$3.000	\$2.157	This funding provides equitable sharing payments to foreign countries, and other federal, state and local law enforcement agencies participating in Secret Service seizure investigations.
H. Services of Experts and Consultants	\$0.015	\$0.050	\$0.075	\$0.002	Funding is for hiring experts to review bank records and other documentary evidence associated with highly complex financial fraud investigation and forfeitable assets.
					<b>INCREASE BY \$.300M (Approved 5/4/2010)</b>
					<b>DECREASED BY \$.300 (Approved 6/1/10)</b>

**U.S. SECRET SERVICE – FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
I. Reimburse State & Locals - Joint Operations	\$1.614	\$1.897	\$1.801	\$1.801	To fund overtime of local law enforcement personnel who support and participate in financial Secret Service investigations.
					<b>INCREASE BY \$800.00 (Approved 9/30/10)</b>
	\$0.140	\$0.112	\$0.100	\$0.092	To support equipment and training expenses related to task force operations, including cell phone monthly usage and publication costs associated with the Identity Theft Project.
<b>Subtotal, Reimburse State &amp; Local - Joint Operations</b>	<b>\$1.754</b>	<b>\$2.009</b>	<b>\$1.901</b>	<b>\$1.893</b>	
J. Data Systems, Training, Contracting for Services					
• FASTRAK Support	\$0.300	\$0.400	\$0.200	\$0.200	To cover cost associated with software upgrades, maintenance and hiring contractor assistance to perform maintenance functions.
• Training	\$0.300	\$0.524	\$0.450	\$0.444	Funding is for EOAF and Secret Service sponsored training initiatives, and basic asset forfeiture and managerial and supervisory training, as well as the procurement of supplies and graphics used in training classes. The funds are to be used solely for training expenses necessary and directly related to forfeiture.
• Contractor Personnel	\$1.400	\$1.361	\$1.500	\$1.500	This will fund Secret Service's contract for technical support related to the Asset Forfeiture Program.
• Treasury Computer Forensics Program (formerly CIS)	\$1.203	\$0.433	\$0.564	\$0.564	The requested funding will support the USSS' portion of the joint ICE/IRS-CI/USSS Computer Forensic Program development and training.
					<b>INCREASE BY \$24K (Approved 3/4/10) Transferred from IRS</b>
<b>Subtotal, Data Systems, Training, Contracting for Services</b>	<b>\$3.203</b>	<b>\$2.718</b>	<b>\$2.714</b>	<b>\$2.708</b>	
<b>SUBTOTAL (MANDATORY)</b>	<b>\$19.412</b>	<b>\$27.259</b>	<b>\$106.320</b>	<b>\$103.662</b>	

**U.S. SECRET SERVICE – FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
<b><u>SUPER SURPLUS EXPENSES:</u></b>					
• Major Case Funding	\$1.000	\$1.000	\$1.300	\$1.300	Funding will be used to support investigative travel, purchase/lease of equipment, including computer forensic ter-storage units, short term lease of undercover facilities, and other additional costs associated with the development of designated major cases with significant seizure potential, often targeting large criminal enterprises.
• FIRS - Bank Secrecy Act Searching	\$0.000	\$0.000	\$0.850	\$0.850	Funding will be used to create a comprehensive, integrated system for the collection and analysis of BSA data specifically catered to the needs and purposes of the US Secret Service. This will allow investigators to discover trends and develop leads on criminal activity that would otherwise not be identified.
• Cyber Investigations Section	\$0.425	\$0.396	\$0.525	\$0.525	Funds will be used to continue to expand a US Secret Service initiative focusing on covert Internet operations that will collect information, analyze data, and identify suspects. Subsequently, a group of highly trained USSS special agents will utilize this information to infiltrate, engage in undercover transactions, and ultimately apprehend primary members / organizers of groups that are conducting credit card/bank fraud, identity theft, and computer network intrusions. This initiative will focus on internationally based targets that have previously been difficult to suppress.
• Wireless Tracking Initiative	\$1.200	\$0.315	\$1.500	\$1.483	This request for funding supports the costs associated with the continuation and expansion of the Secret Service's Wireless Tracking Program, including the upgrade of existing and purchase of new wireless tracking vehicles, training classes, pen register fees, and other equipment and license costs for Electronic Crimes Task Forces. The initiative also contains a research and development component that will be supported by funding.
• Cyber Forensics Contractual Support	\$0.000	\$0.000	\$0.100	\$0.100	To support the United States Secret Service (USSS) Cyber Investigation Section (CIS) initiative focusing on covert Internet operations specializing in malware and data collection, analysis and attribution. A highly specialized forensic company, strategically placed with high level visibility into private/public networks, will support CIS and share information gleaned through their contacts to solidify USSS investigations and offer surge ability in the case of large scale intrusions.
• Treasury Obligations Section	\$0.000	\$0.000	\$0.515	\$0.497	The Counterfeit Detection Training Conference will support all domestic U.S. Secret Service field office personnel who are responsible for processing and classifying counterfeit currency received from financial institutions and law enforcement in their jurisdictions. The primary goal of this conference would be to provide current information and training as well as an open forum to discuss trends and any counterfeit related issues being recognized by field office personnel. (\$55k)  The purchase of cutting edge, automated forensic analyst equipment (3) for currency examination will produce for more quantitative and precise sampling and results, leading to enhance investigations and much more definitive opinions for court testimony. (\$480k)
• Cyber Assurance (Security & Evaluation Implementation)	\$0.000	\$0.000	\$0.250	\$0.250	Through this initiative, the USSS will put in place safe security techniques for the Investigative Warehouse in order to minimize potential cyber security attacks. An evaluation will provide a risk/needs assessment, as well as recommend specific techniques for implementing cyber security. This will position the Investigative Warehouse for a successful Certification & Accreditation. This is a single year initiative.

**U.S. SECRET SERVICE – FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
• Field Operational Support	\$0.350	\$0.400	\$0.500	\$0.400	Funding will be used to purchase up-to-date equipment (hardware and software) not readily available to field personnel to support field operations involving highly technical investigations. The Secret Service maintains an inventory of hardware/software ready for deployment to support field operations (NAS units, Fireflies, Lacie Drives, Laptops, Servers, Firewalls, switches, routers, Mini-storage, etc...). The inventory provides for rapid deployment and cost-effective recycling of existing equipment. Funding will also improve the current distributed networking technology architecture through the development and distribution of efficient hardware and software.
• Investigative Data Warehouse	\$0.850	\$0.250	\$0.150	\$0.150	Funding will be used to continue to replace the hardware/software used to support the day-to-day activities of the investigative/forensic community. Much of the equipment (servers, switches, etc...) is currently out-of-date and needs to be refreshed. The initiative will target the most critical equipment first while attempting to recycle less critical equipment.
• Cellphone Forensics Training	\$0.000	\$0.340	\$0.300	\$0.296	Funding will be used to purchase equipment and training services for cell phone forensics training for USSS's Computer Investigative Specialists. Training will include both basic and advanced courses. As the capabilities of cell phones/hand-held devices expand and become increasingly more sophisticated, it is critical for law enforcement to establish the capability to seize, examine, and analyze the newest technologies.
• Cell Phone Forensics Facility at Tulsa	\$0.600	\$0.296	\$0.300	\$0.298	Funding will be used to cover the overhead costs of the lab facility itself, as well as equipment and supplies needed for the lab. Equipment is need for both investigative forensic analysis and cutting edge research and development.
• Cyber Protection & Investigation	\$0.000	\$0.000	\$12.000	\$11.913	Funding for technology and training associated with the enhancement and deployment of Cyber Advance, Mobile Wireless Perimeter Protection, and the Cyber Intelligence Section to fulfill the protective mission in the face of rapidly advancing cyber technology.
<b>SUBTOTAL (SUPER SURPLUS)</b>	<b>\$4.425</b>	<b>\$2.997</b>	<b>\$18.290</b>	<b>\$18.062</b>	
<b>TOTAL USSS</b>	<b>\$23.837</b>	<b>\$30.256</b>	<b>\$124.610</b>	<b>\$121.724</b>	

**U.S. COAST GUARD – FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt. (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
<b>MANDATORY EXPENSES:</b>					
A. Seizure Investigative Costs & Asset Management					
• Incremental Unit Expenses: 31 U.S.C. 9703	\$0.283	\$0.713	\$1.250	\$0.959	Funding will support Coast Guard Units who engage in seizure enforcement activities. Funding will also offset costs of equipment, training and various joint and pulse operations with other Federal Law Enforcement Agencies and international partners related to forfeiture and seizure.
					<b>MID-YEAR INCREASE: \$.250 (Approved 5/4/10)</b>
• Personnel Expenses: 31 U.S.C. 9703 (a)(1)	\$0.115	\$0.129	\$0.150	\$0.135	Funds for salary, travel, training and equipment costs for the Forfeiture Manager of the USCG. The position title will be Asset Forfeiture Program Specialist at a salary of GS-0301-13. This position is 100% dedicated to Asset Forfeiture Management for the US Coast Guard.
<i>Subtotal Seizure Investigative Costs &amp; Asset Management</i>	<i>\$0.398</i>	<i>\$0.842</i>	<i>\$1.400</i>	<i>\$1.094</i>	
<b>SUBTOTAL (MANDATORY)</b>	<b>\$0.398</b>	<b>\$0.842</b>	<b>\$1.400</b>	<b>\$1.094</b>	



**U.S. COAST GUARD -- FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt. (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
<b><u>SUPER SURPLUS EXPENSES:</u></b>					
• ION SCANS	\$0.000	\$0.000	\$1.350	\$1.288	Funds will be used to purchase IONSCANS for USCG cutters and Law Enforcement Detachment Teams. The IONSCANS detect and identify traces of explosives and narcotics on people, equipment, and vessels exposed to such substances. Funding provided for half of the requested amount.
• Law Enforcement Support Kit	\$0.000	\$0.000	\$0.810	\$0.809	Funds will be used to purchase Law Enforcement Support Kits for major cutters and Law Enforcement Detachment Teams. The kits will standardize supplies throughout the fleet and provide the necessary equipment to conduct boardings and search for narcotics on suspected vessels. Funding provided for half of the requested amount.
• Portable X-Ray System	\$0.000	\$0.000	\$1.080	\$0.989	Funds will be used to purchase the portable X-ray systems for USCG Cutters and Law Enforcement Detachment Teams. The system will aid boarding teams on counter-narcotics boardings by allowing for non-intrusive searches of spaces. Funding provided for half of the requested amount.
<b>SUBTOTAL (SUPER SURPLUS)</b>	<b>\$0.000</b>	<b>\$0.000</b>	<b>\$3.240</b>	<b>\$3.086</b>	
<b>TOTAL USCG</b>	<b>\$0.398</b>	<b>\$0.842</b>	<b>\$4.840</b>	<b>\$4.180</b>	

**FEDERAL LAW ENFORCEMENT TRAINING CENTER – FY 2010 FINANCIAL PLAN**

Expense Category	FY 2008 Final Obl. (\$ Millions)	FY 2009 Final Obl. (\$ Millions)	FY 2010 Appr. Amt. (\$ Millions)	FY 2010 Final Obl. (\$ Millions)	Description/Comments
<b>MANDATORY EXPENSES:</b>					
J. Data Systems, Training, Contracting for Services • Training	\$0.240	\$0.300	\$0.365	\$0.345	Funding is for continued training conducted by the Federal Law Enforcement Training Center that is directly related to the Asset Forfeiture Program. Staffing remains the same at two positions. (b)(5)
<b>SUBTOTAL (MANDATORY)</b>	<b>\$0.240</b>	<b>\$0.300</b>	<b>\$0.365</b>	<b>\$0.345</b>	



**Homeland  
Security**

May 8, 2012

The Honorable Michael T. McCaul  
U.S. House of Representatives  
Washington, DC 20515

Dear Representative McCaul:

Thank you for your February 29, 2012 letter to Secretary Napolitano requesting additional records related to a FOIA request made by Albert Krachman, an attorney with Blank Rome, LLP, in Washington, DC, on behalf of Lynntech, Inc., a constituent company. Albert Krachman is seeking information pertaining to the administration, funding, and subsequent defunding of the Department of Homeland Security's (DHS) Portable BioDetector Project under DHS Contract No. HSHQDC-09-0119. It may be helpful to review the processing of this FOIA request.

On August 2, 2011, the DHS Management Directorate received the subject request filed by Mr. Krachman. On August 5, 2011, the DHS Management Directorate tasked the search for responsive documents to the Science and Technology Directorate (S&T), which conducted a records search and subsequently issued an interim response totaling 163 pages. Of those pages, S&T released 73 in their entirety and 72 in part. The remaining 18 pages were withheld in full pursuant to Title 5 U.S.C. § 552 (b)(5) and (b)(6).

On November 17, 2011, Albert Krachman appealed the withholding determinations in the interim response. The DHS FOIA Office acknowledged receipt of the appeal on November 30, 2011 and, on December 16, 2011, forwarded the appeal to the United States Coast Guard Administrative Law Judge (ALJ), who adjudicates appeals for the FOIA Office. The appeal is and will remain under the purview of the ALJ until the ALJ renders its decision.

On behalf of your constituent company, Lynntech, Inc., you have asked that DHS provide to you all the documentation Lynntech, Inc., has requested and in a format free of redactions. Although FOIA and the Privacy Act generally do not authorize special access by Members of Congress, those laws do authorize the release of records to the Chairman of a committee or subcommittee with jurisdiction over the subject matter of the request. (See 5 U.S.C. §§ 552(d) and 5 U.S.C.a(b)(9)). In the instant case, the request has been made on behalf of a constituent and not a committee or subcommittee and so, to the extent that the records requested exist within DHS records holdings, the Department may release them only as authorized by the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and the Privacy Act 5 U.S.C. § 552a.



Thank you again for your letter. Please be assured that your constituent's request is appropriately in the appeal process and that we will issue our final response to Albert Krachman's request in a timely manner. Should you need additional assistance, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock", with a stylized flourish at the end.

Nelson Peacock  
Assistant Secretary for Legislative Affairs



**Homeland  
Security**

April 2, 2012

The Honorable Michael T. McCaul  
Chairman  
Committee on Homeland Security  
Subcommittee on Oversight,  
Investigations and Management  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman McCaul:

Thank you for your letter stating your support for a robust and risk-informed Quadrennial Homeland Security Review (QHSR).

Your letter emphasizes the need for continued integration of risk information into the Department's strategic planning and decision-making processes. DHS fully concurs with this approach and has worked to make this a reality since completion of the first QHSR.

As you know, the Fiscal Year 2012 DHS Appropriations Act authorized the Secretary to transfer the risk management and analysis functions currently performed by the Office of Risk Management and Analysis (RMA) to the Office of Policy in 2012. As the Office of Policy will lead the Department's efforts to conduct the next QHSR, this transfer will enhance and synchronize the Department's risk assessment and strategic planning functions, and aid in ensuring that risk analysis effectively informs strategy development and strategic choice through the QHSR.

Under the schedule set forth in the *Implementing Recommendations of the 9/11 Commission Act of 2007*, the Department will conduct its next quadrennial review in 2013. Because the first QHSR set a durable framework of homeland security missions, the next quadrennial review can focus on a more extensive examination of the security environment, including strategic risk and potential future trends and shocks. The next QHSR will also focus on a deeper review of a few key challenges within homeland security, including a deeper look at the relative risk reduction benefits of different strategic approaches to these challenges. As a result, the next QHSR will reflect a greater integration of risk analysis into all stages of the quadrennial review, as you have requested and as was previously recommended by the Government Accountability Office (GAO) in their review of the first QHSR. The Department also acknowledges, is committed to, and is currently planning for a more fulsome stakeholder engagement and outreach effort in the next QHSR as you have requested and as GAO previously recommended.

Finally, in response to your comments regarding the varying frameworks and definitions in use within the Department, DHS views the initial QHSR as establishing the foundation for a unified understanding of the missions and activities of DHS and the homeland security enterprise.

Implementation of the QHSR is a task that DHS continues to pursue, precisely because DHS shares your perspective that unity of vision leads to unity of effort. DHS has made significant progress in this area, with a range of products building on and informed by the strategic framework established in the 2010 QHSR. These include, among others, the Department's FY 2012 budget request, the *FY 2012-2016 Future Years Homeland Security Plan*, the *FY 2010-2012 Annual Performance Report and Plan*, and the recently published *FY 2012-2016 DHS Strategic Plan*. Within DHS components, consistency with the QHSR can be seen in the *2011-2014 FEMA Strategic Plan*, which describes the cascade from the *National Security Strategy* through the 2010 QHSR down to the FEMA Administrator's Intent Priorities, as well as the 2010-2014 ICE Strategic Plan, which draws its four priorities from the QHSR mission structure.

The Department has begun planning for the next QHSR, paying close attention to your concerns and other opportunities for improvement, and we look forward to working with you to execute this second quadrennial review. If I may be of further assistance, please contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock", with a stylized, flowing script.

Nelson Peacock  
Assistant Secretary for Legislative Affairs



**Homeland  
Security**

JUN 07 2012

The Honorable Michael T. McCaul  
U.S. House of Representatives  
Committee on Homeland Security  
Washington, DC 20515

Dear Chairman McCaul:

Thank you for your letter dated May 17, 2012, in reference to employee morale at the Department of Homeland Security (DHS). We are committed to making DHS one of the best places to work in the federal government by prioritizing employee engagement, supporting a unified One DHS strategy, and strengthening the leadership skills and capacity of all supervisors and managers within DHS.

We know that many of the best ideas come from employees at all levels of our organization. In fact, many of the initiatives we are implementing across the Department to streamline operations, increase collaboration, and make the most of limited resources, are based directly on employee feedback.

We look forward to engaging stakeholders and soliciting employee input as we work to improve employee morale and engagement within DHS. We thank you for your continued support.

Yours very truly,

A handwritten signature in cursive script that reads "Catherine V. Emerson".

Catherine V. Emerson  
Chief Human Capital Officer





**Homeland  
Security**

June 28, 2012

The Honorable Peter T. King  
Chairman  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman King:

Thank you for your recent letter supporting Governor Cuomo's request for a National Special Security Event (NSSE) designation for the 2012 Presidential Debate at Hofstra University on October 16. After careful consideration by the NSSE Working Group, the Secretary determined that this event will not be designated as an NSSE.

Although the 2012 Presidential Debate at Hofstra University does not qualify as an NSSE, we have encouraged Governor Cuomo to submit this event to the National Special Events Data Call, which is conducted by the Special Events Program under the U.S. Department of Homeland Security's Office of Operations Coordination and Planning. The data call captures information that is used to conduct an analysis of the event that results in the assignment of a Special Event Assessment Rating (SEAR). The SEAR designation is used by agencies within the Federal Government to determine the appropriate scope of support for the event, and the data call provides detailed information that enhances situational awareness.

Thank you again for your letter. I look forward to continuing to work with you on these issues in the future. Should you need additional assistance, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in blue ink, appearing to read "N. Peacock".

Nelson Peacock  
Assistant Secretary for Legislative Affairs

Enclosure





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

**Homeland  
Security**

July 19, 2012

The Honorable Michael McCaul  
Chairman  
Subcommittee on Oversight,  
Investigations, and Management  
Committee on Homeland Security  
U. S. House of Representatives  
Washington, DC 20515

Dear Chairman McCaul:

This responds to your letter to Secretary Napolitano regarding management integration and oversight at the Department of Homeland Security (DHS). I appreciate the opportunity to discuss our efforts to integrate management functions and to continue to build One DHS.

Progress must be viewed through the full spectrum of management issues, factoring in each progressive step, some of which will be incremental, as part of the continuing integration of an organization as large and complex as DHS. Over the past 18 months, DHS has made considerable progress to address the 31 GAO Outcomes and remains committed to sustaining momentum over the coming years. We have created a solid framework through corrective action plans and a strategy that integrates our people, processes and structures. The progress that we have achieved since the last report is the best evidence that both our strategy and our efforts are appropriately focused.

On June 15, 2012, the Under Secretary for Management submitted the Department's third comprehensive report to the GAO on its integration strategy. This update provided more evidence to support the significant progress DHS has made in reducing the number of outstanding GAO Outcomes.

The most significant finding contained in the June 2012 update is that clear and measurable progress has been made to increase the number of GAO Outcomes that now fall in the "Fully" and "Mostly Addressed" categories. As of the June 2012 update, 17 of the 31 Outcomes are now "Fully" or "Mostly Addressed," up from 7 in December 2011. We expect this trend to continue, as our goal is to make significant progress against all 31 Outcomes over the coming months. The progress shown in this update demonstrates that

DHS is continuously improving the content and quality of each bi-annual update so all Departmental management functions can be eligible to be removed from the “high risk” list.

We appreciate the acknowledgement in your June 4<sup>th</sup> letter of our efforts to improve oversight of acquisition programs across the Department. The Department is committed to continued improvement through establishment of Centers of Excellence for Acquisition and Program Management, the Decision Support Tool, and intensive portfolio reviews.

Through our Centers of Excellence initiative, for example, we are now providing training workshops on cost estimating to address weaknesses identified by the GAO. In addition, we continue to mature the Decision Support Tool to give leadership greater insights into the health of our major programs. For example, as of this month, leadership can now access a “program snapshot” of major programs’ health indicators, such as cost, schedule, and performance.

While the Department is pleased with its progress to achieve One DHS, we acknowledge there is still work ahead. We value our partnership with GAO and will continue to leverage their expertise and advice over the coming months.

Thank you again for the opportunity to respond to these important issues. Should you need additional assistance, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock", with a stylized, flowing script.

Nelson Peacock  
Assistant Secretary for Legislative Affairs



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

# Homeland Security

July 24, 2012

The Honorable Peter T. King  
Chairman  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your recent letter inquiring about the circumstances under which a visa to visit the United States was granted to Egyptian parliamentarian Hany Noureldin Abobakr Sedik, known in Egypt as Hani Nour Eldin. In your letter, you raised a number of questions, and I have responded to each, in turn, below.

Please note that, according to the provisions of section 222(f) of the *Immigration and Nationality Act* (INA), visa records are considered confidential and may only be used for the formulation, amendment, administration or enforcement of the immigration, nationality and other law of the United States. Given that you are requesting these records as the Chair of a Committee under whose jurisdiction these matters fall, the Department of State has determined that your request conforms to the requirements of section 222(f) and has therefore provided the information related to Mr. Sedik's recent visa application. Because this letter contains protected information, please ensure that access to and use of such information is solely for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States under INA 222(f) and please take appropriate measures to protect it from unauthorized disclosure.

**1. What U.S. Government department or agency sponsored Eldin's visa application, and for what reason?**

Mr. Eldin traveled as an Egyptian Parliamentarian from the Construction and Development Party in order to attend a Department of State-sponsored program in Washington, D.C. He was one of eight parliamentarians selected by the U.S. Embassy to attend a program designed for newly elected Egyptian leaders to meet with U.S. federal and congressional leaders, business leaders, and other think tank representatives.

**2. What steps did that department or agency take to trace Eldin's background? Was it aware of his membership in the Islamic Group, or not?**

The Department of State collected Mr. Eldin's personal and family information, travel history, previous and present work, education, and training information, and required Mr. Eldin to answer extensive security and background questioning. His application was also reviewed and cleared by the U.S. Immigration and Customs Enforcement Visa Security Unit. The State Department requested an interagency Security Advisory Opinion (SAO) for further review of his background and possible affiliations. When the interagency SAO process was completed, there was no derogatory information discovered on Mr. Eldin. The Intelligence Community also vetted Mr. Eldin and no derogatory information was found.

**3. What information, if any, did the department or agency sponsoring Eldin's visit share with the Department of Homeland Security regarding Eldin's membership in a designated terrorist organization and his pending visit to the United States?**

The Department of State made available to the Department of Homeland Security (DHS) the itinerary and biographic details for the delegates scheduled to travel to the United States. Document and visa information was made available to DHS representatives through the use of a State Department database, the Consular Consolidated Database. The SAO request indicated only that Mr. Eldin was a member of the Construction and Development political party, and that some members of that party are formerly members of the Gama'a Islamiya (Islamic Group) organization, which is a U.S.-designated Foreign Terrorist Organization.

**4. What rationale did Customs and Border Protection apply to allow Eldin's admittance into the United States? And, when entering the country, did Eldin undergo secondary inspection?**

Mr. Eldin's biographical data was received by U.S. Customs and Border Protection (CBP) prior to his flight departure via the Advance Passenger Information System (APIS) and it was entered into CBP's Automated Targeting System (ATS). Mr. Eldin's biographical data was processed in ATS through CBP's Pre-Departure program. APIS and ATS vetting of Mr. Eldin's biographical data did not result in an alert for any possible types of derogatory information.

APIS and ATS vetting allow CBP's National Targeting Center to:

- screen passenger and related information prior to a passenger arriving in the United States;
- respond to terrorism-related alerts and provide time-sensitive research; and
- provide support for any issues related to international passengers at U.S. ports of entry.

Upon arrival, he was identified as a member of an Egyptian delegation applying for admission as a visitor for official business. CBP conducted a primary inspection, which includes validation of immigration documents, interview, biometric collection, and biographic and biometric systems query checks. There was no derogatory information discovered during the course of primary inspection, and Mr. Eldin was not referred to secondary inspection. He was deemed admissible to the United States.<sup>1</sup>

**5. What information, if any, was relayed to the United States Secret Service (USSS) in advance of this Islamic Group member's appointment at the White House? Did the USSS express any security concerns about the location of this meeting?**

In advance of the delegation's June 19 meeting on the White House complex, delegation members provided the standard information for foreign nationals, including full name, date of birth, passport number, citizenship, gender, and place of residence. USSS processed that information pursuant to its established protocol.

**6. During his visit to the United States, did Eldin engage in any activities which might constitute material support for terrorism under 18 U.S.C. § 2339B?**

We are not aware of any such activity during his visit. In any event, we would refer any such matter to the Department of Justice, which is responsible for enforcement of 18 U.S.C. § 2339B.

**7. What policies and procedures are in place regarding interagency notifications of visits of members of designated terrorist organizations to the United States?**

Pursuant to 212(a)(3)(B)(i)(V) of the INA (8 U.S.C. § 1182(a)(3)(B)(i)(V)), a member of a designated terrorist organization is inadmissible to the United States and would require a waiver or exemption of inadmissibility pursuant to 212(d)(3)(A) or (B) of the INA (8 U.S.C. § 1182(d)(3)(A) or (B)) in order to be admitted to the United States.

**8. What is the position of the Department of Homeland Security regarding any potential custodial transfer, or release, of Omar Abdel Rahman?**

Omar Abdel Rahman is in federal custody. We refer you to the Department of Justice for more information on his status.

---

<sup>1</sup> The *Immigration and Nationality Act* (INA) defines the grounds of inadmissibility in section 212(a) (8 U.S.C. § 1182).



Again, thank you for your letter. I hope to continue fostering a close working relationship with you on this issue and other homeland security matters. Should you need additional assistance, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Nelson Peacock  
Assistant Secretary for Legislative Affairs



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

**Homeland  
Security**

July 24, 2012

The Honorable Peter T. King  
Chairman  
Committee on Homeland Security  
U. S. House of Representatives  
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your June 27 letter to Secretary Napolitano on the draft *National Planning Frameworks (Frameworks)*, a component of *Presidential Policy Directive / PPD-8: National Preparedness*. The Department of Homeland Security fully recognizes the importance of the Intelligence and Information Sharing core capability as critical to the well-being of the United States. We agree that informed first responders and law enforcement officers are essential to America's security and resilience. You may be assured that your concerns regarding intelligence and information sharing are being taken into consideration as the *Frameworks* reach completion and prior to their final submission to the White House by November 1, 2012.

Identical responses have been sent to Chairman Bilirakis and Representative Turner, who co-signed your letter. Thank you again for your support. Should you require further assistance, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock".

Nelson Peacock  
Assistant Secretary for Legislative Affairs



**Homeland  
Security**

January 25, 2013

The Honorable Michael McCaul  
Chairman, Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman McCaul:

Thank you for your letter to the Under Secretary for Management, requesting information on conferences funded by the Department of Homeland Security (DHS). Please find the enclosed document, which contains data responsive to your request.

DHS is the third largest federal agency and the largest law enforcement agency in the Federal Government. The DHS workforce consists of more than 240,000 law enforcement agents, officers, active-duty military personnel, and men and women on the frontlines who put their lives at risk every day to protect our country from threats to the homeland, securing our land, air, and maritime borders, enforcing our immigration laws, and responding to natural disasters. These employees are stationed in every state and in more than 75 countries around the world. Training events and workshops are critical to bringing our geographically dispersed workforce together and ensuring that our personnel are fully equipped and prepared to carry out their missions.

In order to execute our missions, and to do so in an efficient and effective manner, DHS also offers significant training and technical assistance to state, local, and tribal law enforcement and first responders to build expertise and capabilities across the country. Section 102(c) of the *Homeland Security Act* (6 U.S.C. § 112(c)) requires the Secretary to coordinate with state and local governments, and the private sector, with respect to homeland security issues. Among other responsibilities, the Secretary is required to coordinate with such entities to ensure adequate planning, equipment, training, and exercise activities. As demonstrated during the response to recent natural disasters including the devastating tornadoes in the South and Midwest and Hurricanes Irene and Sandy, a well-trained cadre of first responders is critical to ensuring an effective response, helping to save lives, and minimize damage. Time and time again, we have also seen the value of our state, local, and tribal law enforcement training in disrupting terrorist plots and other crimes.

DHS is dedicated to being a responsible steward of taxpayer dollars and is fully committed to using our resources effectively and efficiently to support frontline operations.

To that end, in 2009, Secretary Napolitano launched the Department-wide Efficiency Review (ER) to foster a culture of responsibility, accountability, and fiscal discipline. Over the past four years, we have identified over \$4 billion in cost avoidances by cutting costs, sharing resources across Components, and consolidating and streamlining operations wherever possible.

One of the Department's first ER initiatives focused on maximizing the use of Government office space and facilities for training events and meetings in lieu of renting more costly meeting space. Furthermore, DHS has established additional conference and travel policies and controls to ensure conferences are cost-effective and to ensure conference attendance is driven by critical mission requirements. These include:

- Establishing additional conference-related responsibilities for the CFO and Components.
- Incorporating requirements to use government facilities, cost-effective alternatives to commercial facilities, and limiting the number of DHS attendees to conferences – consistent with the Efficiency Review travel guidance.
- Amending existing guidance by adding a section on the authority to collect conference fees from non-federal participants, including the statutory reporting requirement.
- Better defining DHS requirements to justify, document, and report conference-related expenses.
- Adding special reminders for travel approvers as to certain things for which they should be checking, such as use of non-contract carriers, deductions of per diem when meals are provided at conferences, and reasonableness of expenses requested in the authorization process.

In October 2011, DHS conducted an assessment to confirm appropriate conference policy and internal controls were in place Department-wide. The Chief Financial Officer identified 18 key controls already in place within Department policy and asked each Component to assess and certify those key controls. The results of our assessment and ongoing conference reviews show that the Department has improved the efficiency and cost effectiveness of its conference-related expenses and activities, consistent with DHS Efficiency Review initiatives on travel and facilities. To reinforce these controls, during the Fall of 2012, DHS issued a new conference policy (enclosed) that established further standards for conferences and requires regular reporting on conference spending, further increasing transparency and accountability.

These policy changes, combined with the additional review process implemented in response to OMB M-11-35 ("Eliminating Excess Conference Spending and Promoting Efficiency in Government"), have generated cost-avoidances within DHS Components and offices. More training events are now being held locally and Components and offices are increasing the use of video teleconferencing in lieu of in-person meetings while also strengthening internal management oversight and controls.

We will continue to monitor training events and workshops across the Department and will work with Components and offices to ensure that all resources are spent responsibly and in support of critical mission requirements.

If you have any questions or need further information, please do not hesitate to contact me at (202) 447-5890.

Respectfully,



Nelson Peacock  
Assistant Secretary for Legislative Affairs

Enclosures:

- List of Conferences
- DHS Conference Controls Policy
- DHS Conference Planning and Attendance Guidelines
- DHS Efficiency Review Travel and Conference Directive
- DHS Travel and Conference information site
- DHS Acquisition Memorandum: Eliminating Excess Conference Spending
- OMB Memorandum: Eliminating Excess Conference Spending and Promoting Efficiency in Government





**Homeland  
Security**

November 16, 2012

The Honorable Michael T. McCaul  
Chairman  
Subcommittee on Oversight, Investigations and Management  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman McCaul:

Thank you for your recent letter to Secretary Napolitano regarding the 2012 Formula 1 United States Grand Prix, hosted at the Circuit of the Americas in Austin, Texas, on November 18, 2012. I appreciate your interest in the security of this event.

On October 31, the Department of Homeland Security (DHS) received a letter from Governor Rick Perry formally requesting that this event be designated as a National Special Security Event (NSSE). After careful consideration, DHS determined this event will not be designated as an NSSE; however, DHS has initiated a number of actions in response to requests for assistance including risk assessments, gap analysis, and direct support to state and local authorities.

DHS is providing assistance with enhanced cargo screening, infrastructure security assessments, increased passenger screening at the Austin-Bergstrom International Airport, and the deployment of Visible Intermodal Prevention and Response teams in support of the event. The Department will continue to assess the threat environment to determine if emerging threats warrant changes to our operations, and I assure you that we will work diligently to assist with any additional requests for assistance that we receive.

We wish you great success with this event and look forward to continuing to work with you on these issues in the future. Should you need additional assistance, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, reading "Nelson Peacock".

Nelson Peacock  
Assistant Secretary for Legislative Affairs

cc: The Honorable David S. Adams, Assistant Secretary for Legislative Affairs, Department of State  
The Honorable Robert Mueller, Director, FBI



# Homeland Security

June 4, 2013

The Honorable Peter T. King  
Chairman  
Subcommittee on Counterterrorism and Intelligence  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman King:

Thank you for your recent letter regarding the Department of Homeland Security's agreement with the United Arab Emirates for a U.S. Customs and Border Protection preclearance operation in Abu Dhabi. To best address your concerns, we have answered each of your questions in the enclosed white paper.

Again, thank you for your letter. The cosigners of your letter will each receive a separate, identical response. I hope to continue to foster a close working relationship with you on this issue and other homeland security matters. Should you need additional assistance, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, reading "Brian de Vallance".

Brian de Vallance  
Acting Assistant Secretary for Legislative Affairs

Enclosure



**Homeland  
Security**

June 7, 2013

The Honorable Michael T. McCaul  
Chairman  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman McCaul:

Thank you for your recent letter to Secretary Napolitano and Attorney General Holder requesting details about the Saudi student who was an original person of interest in the Boston Marathon bombing. As reflected in a briefing to Committee on Homeland Security staff on April 25, 2013, the "original" person of interest was an individual named Abdul Rahman Al-Harbi. Mr. Al-Harbi is a student and holds valid immigration status.

However, a separate, unconnected case involving a Saudi national student was reported in the press around the same time period. (b)(6) came to the United States on a valid F-1 visa, however, he did not comply with the terms of his nonimmigrant admission. He was arrested by U.S. Immigration and Customs Enforcement on April 16, 2013 and is awaiting an immigration hearing. The arrest of (b)(6) is not connected to the Boston bombing, nor does he have any suspected ties to terrorist or criminal activity. ICE will make appropriate determinations on next steps following (b)(6) immigration proceedings.

Thank you again for your letter. This response has been coordinated with the Department of Justice and the other Members of Congress who co-signed your letter will receive identical responses. Should you have additional questions please contact the DHS Office of Legislative Affairs at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Brian de Vallance".

Brian de Vallance  
Acting Assistant Secretary for Legislative Affairs





**Homeland  
Security**

June 7, 2013

The Honorable Candice S. Miller  
U.S. House of Representatives  
Washington, DC 20515

Dear Representative Miller:

Thank you for your recent letter to Secretary Napolitano and Attorney General Holder requesting details about the Saudi student who was an original person of interest in the Boston Marathon bombing. As reflected in a briefing to Committee on Homeland Security staff on April 25, 2013, the "original" person of interest was an individual named Abdul Rahman Al-Harbi. Mr. Al-Harbi is a student and holds valid immigration status.

However, a separate, unconnected case involving a Saudi national student was reported in the press around the same time period. (b)(6) came to the United States on a valid F-1 visa, however, he did not comply with the terms of his nonimmigrant admission. He was arrested by U.S. Immigration and Customs Enforcement on April 16, 2013 and is awaiting an immigration hearing. The arrest of (b)(6) is not connected to the Boston bombing, nor does he have any suspected ties to terrorist or criminal activity. ICE will make appropriate determinations on next steps following (b)(6) immigration proceedings.

Thank you again for your letter. This response has been coordinated with the Department of Justice and the other Members of Congress who co-signed your letter will receive identical responses. Should you have additional questions please contact the DHS Office of Legislative Affairs at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Brian de Vallance".

Brian de Vallance  
Acting Assistant Secretary for Legislative Affairs



## Homeland Security

June 7, 2013

The Honorable Peter T. King  
Chairman  
Subcommittee on Counterterrorism  
and Intelligence  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman King:

Thank you for your recent letter to Secretary Napolitano and Attorney General Holder requesting details about the Saudi student who was an original person of interest in the Boston Marathon bombing. As reflected in a briefing to Committee on Homeland Security staff on April 25, 2013, the "original" person of interest was an individual named Abdul Rahman Al-Harbi. Mr. Al-Harbi is a student and holds valid immigration status.

However, a separate, unconnected case involving a Saudi national student was reported in the press around the same time period. (b)(6) came to the United States on a valid F-1 visa, however, he did not comply with the terms of his nonimmigrant admission. He was arrested by U.S. Immigration and Customs Enforcement on April 16, 2013 and is awaiting an immigration hearing. The arrest of (b)(6) is not connected to the Boston bombing, nor does he have any suspected ties to terrorist or criminal activity. ICE will make appropriate determinations on next steps following (b)(6) immigration proceedings.

Thank you again for your letter. This response has been coordinated with the Department of Justice and the other Members of Congress who co-signed your letter will receive identical responses. Should you have additional questions please contact the DHS Office of Legislative Affairs at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Brian de Vallance".

Brian de Vallance  
Acting Assistant Secretary for Legislative Affairs





## Homeland Security

June 7, 2013

The Honorable Susan W. Brooks  
U.S. House of Representatives  
Washington, DC 20515

Dear Representative Brooks:

Thank you for your recent letter to Secretary Napolitano and Attorney General Holder requesting details about the Saudi student who was an original person of interest in the Boston Marathon bombing. As reflected in a briefing to Committee on Homeland Security staff on April 25, 2013, the "original" person of interest was an individual named Abdul Rahman Al-Harbi. Mr. Al-Harbi is a student and holds valid immigration status.

However, a separate, unconnected case involving a Saudi national student was reported in the press around the same time period. (b)(6) came to the United States on a valid F-1 visa, however, he did not comply with the terms of his nonimmigrant admission. He was arrested by U.S. Immigration and Customs Enforcement on April 16, 2013 and is awaiting an immigration hearing. The arrest of (b)(6) is not connected to the Boston bombing, nor does he have any suspected ties to terrorist or criminal activity. ICE will make appropriate determinations on next steps following (b)(6) immigration proceedings.

Thank you again for your letter. This response has been coordinated with the Department of Justice and the other Members of Congress who co-signed your letter will receive identical responses. Should you have additional questions please contact the DHS Office of Legislative Affairs at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Brian de Vallance".

Brian de Vallance  
Acting Assistant Secretary for Legislative Affairs



## Homeland Security

June 7, 2013

The Honorable Jeff Duncan  
U.S. House of Representatives  
Washington, DC 20515

Dear Representative Duncan:

Thank you for your recent letter to Secretary Napolitano and Attorney General Holder requesting details about the Saudi student who was an original person of interest in the Boston Marathon bombing. As reflected in a briefing to Committee on Homeland Security staff on April 25, 2013, the "original" person of interest was an individual named Abdul Rahman Al-Harbi. Mr. Al-Harbi is a student and holds valid immigration status.

However, a separate, unconnected case involving a Saudi national student was reported in the press around the same time period. (b)(6) came to the United States on a valid F-1 visa, however, he did not comply with the terms of his nonimmigrant admission. He was arrested by U.S. Immigration and Customs Enforcement on April 16, 2013 and is awaiting an immigration hearing. The arrest of (b)(6) is not connected to the Boston bombing, nor does he have any suspected ties to terrorist or criminal activity. ICE will make appropriate determinations on next steps following (b)(6) immigration proceedings.

Thank you again for your letter. This response has been coordinated with the Department of Justice and the other Members of Congress who co-signed your letter will receive identical responses. Should you have additional questions please contact the DHS Office of Legislative Affairs at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Brian de Vallance".

Brian de Vallance  
Acting Assistant Secretary for Legislative Affairs





## Homeland Security

June 7, 2013

The Honorable Richard Hudson  
U.S. House of Representatives  
Washington, DC 20515

Dear Representative Hudson:

Thank you for your recent letter to Secretary Napolitano and Attorney General Holder requesting details about the Saudi student who was an original person of interest in the Boston Marathon bombing. As reflected in a briefing to Committee on Homeland Security staff on April 25, 2013, the "original" person of interest was an individual named Abdul Rahman Al-Harbi. Mr. Al-Harbi is a student and holds valid immigration status.

However, a separate, unconnected case involving a Saudi national student was reported in the press around the same time period. (b)(6) came to the United States on a valid F-1 visa, however, he did not comply with the terms of his nonimmigrant admission. He was arrested by U.S. Immigration and Customs Enforcement on April 16, 2013 and is awaiting an immigration hearing. The arrest of (b)(6) is not connected to the Boston bombing, nor does he have any suspected ties to terrorist or criminal activity. ICE will make appropriate determinations on next steps following (b)(6) immigration proceedings.

Thank you again for your letter. This response has been coordinated with the Department of Justice and the other Members of Congress who co-signed your letter will receive identical responses. Should you have additional questions please contact the DHS Office of Legislative Affairs at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Brian de Vallance".

Brian de Vallance  
Acting Assistant Secretary for Legislative Affairs



# Homeland Security

September 10, 2013

The Honorable Jeff Duncan  
Chairman  
Subcommittee on Oversight and Management Efficiency  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Mr. Chairmam:

Thank you for your recent letter inquiring about the status of a report by the Department of Homeland Security (DHS) to Congress on its integrity efforts.

The Department appreciates the significance of this report, which is required in response to language set forth in Senate Report 112-169 accompanying the *Fiscal Year 2013 DHS Appropriations Act* (P.L. 113-6). The issues identified in the report are of profound importance, and efforts have been made to ensure that Congress is provided accurate and complete information. The report is nearly completed and is anticipated for delivery later this month. Consistent with your request, the report will be provided to the House Committee on Homeland Security. The Department will be pleased to follow up with a Committee staff briefing as desired.

Thank you again for your letter. If you have any further questions or concerns, please feel free to contact the Office of Legislative Affairs at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Brian de Vallance".

Brian de Vallance  
Acting Assistant Secretary for Legislative Affairs



**Homeland  
Security**

JUN 07 2012

The Honorable Michael T. McCaul  
U.S. House of Representatives  
Committee on Homeland Security  
Washington, DC 20515

Dear Chairman McCaul:

Thank you for your letter dated May 17, 2012, in reference to employee morale at the Department of Homeland Security (DHS). We are committed to making DHS one of the best places to work in the federal government by prioritizing employee engagement, supporting a unified One DHS strategy, and strengthening the leadership skills and capacity of all supervisors and managers within DHS.

We know that many of the best ideas come from employees at all levels of our organization. In fact, many of the initiatives we are implementing across the Department to streamline operations, increase collaboration, and make the most of limited resources, are based directly on employee feedback.

We look forward to engaging stakeholders and soliciting employee input as we work to improve employee morale and engagement within DHS. We thank you for your continued support.

Yours very truly,

A handwritten signature in cursive script, reading "Catherine V. Emerson".

Catherine V. Emerson  
Chief Human Capital Officer



Secretary

U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

September 6, 2011

The Honorable Patrick Meehan  
Chairman  
Subcommittee on Counterterrorism and Intelligence  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Representative Meehan:

Thank you for your letter regarding the Department of Homeland Security's role in the analysis, distribution, and response to the cache of information that was collected from Usama Bin Ladin's compound during the successful special forces operation. I have enclosed a paper that provides responses to your specific questions about DHS's involvement.

DHS has worked with our counterterrorism partners throughout the Intelligence Community to keep our homeland security partners informed and ensure that timely, appropriate information is provided to stakeholders. I agree that it is essential that DHS leverage this victory to help keep our stakeholders informed of the current threat. The enclosure details efforts to date.

Thank you again for your letter. I look forward to continuing to work with you on this and other homeland security matters. If I can be of any further assistance please do not hesitate to contact me on (202) 282-(b)(6)

Yours very truly,

A handwritten signature in black ink, appearing to read "Janet Napolitano", with a long horizontal flourish extending to the right.

Janet Napolitano

Enclosure



Homeland  
Security

MAR 8 2013

The Honorable Michael McCaul  
Chairman, Subcommittee on Oversight,  
Investigations, and Management  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman McCaul:

Thank you for your letter of February 20, 2013, recognizing the Department's progress in addressing the issues noted by the Government Accountability Office. Obtaining a clean audit opinion and modernizing the Department's financial management systems using best practices are key priorities for the Department of Homeland Security (DHS) and critical to sustaining our progress and supporting timely access to financial information for strategic decision making.

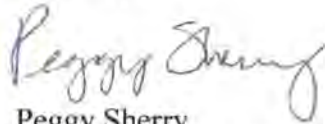
In November 2012, the Department obtained a qualified opinion on all five financial statements. The only remaining qualification on the DHS Balance Sheet is related to the U.S. Coast Guard's general property, plant and equipment (including heritage and stewardship assets). Fiscal Year (FY) 2012 was the first year in which the Department presented all five financial statements for audit, and notably the expanded scope in FY 2012 did not result in any additional qualifications. In FY 2013, the Department is actively pursuing a clean opinion on all five financial statements.

Our Financial Systems Modernization initiative remains a priority for the Department. This initiative will improve the Department's ability to provide current, accurate, and more useful financial information to DHS leaders and stakeholders through expanded business intelligence capabilities and modernizing financial systems where needed. In 2010, my office conducted extensive market research to gather and evaluate lessons learned and best practices from federal and commercial shared service providers that recently completed a financial system implementation. Our research focused on the system implementation phase in agencies across the federal sector.

We continue regular communications with these federal agencies and are working closely with the Office of Management and Budget (OMB) and the Department of the Treasury's Office of Financial Innovation and Transformation (FIT) as they formulate the governmentwide vision and roadmap for financial management systems modernization.

Thank you for your support to make DHS efficient and effective. The Representatives who cosigned your letter will receive separate, identical responses. If we may be of further assistance, please contact Larry Bedker, Director, Financial Management, at (202) 447-(b)(6)

Sincerely,

A handwritten signature in cursive script, appearing to read "Peggy Sherry".

Peggy Sherry  
Chief Financial Officer



MAR 8 2013



Homeland  
Security

The Honorable Jeff Duncan  
U.S. House of Representatives  
Washington, DC 20515

Dear Representative Duncan:

Thank you for your letter of February 20, 2013, recognizing the Department's progress in addressing the issues noted by the Government Accountability Office. Obtaining a clean audit opinion and modernizing the Department's financial management systems using best practices are key priorities for the Department of Homeland Security (DHS) and critical to sustaining our progress and supporting timely access to financial information for strategic decision making.

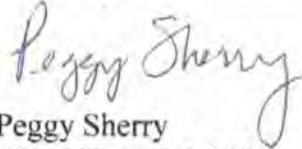
In November 2012, the Department obtained a qualified opinion on all five financial statements. The only remaining qualification on the DHS Balance Sheet is related to the U.S. Coast Guard's general property, plant and equipment (including heritage and stewardship assets). Fiscal Year (FY) 2012 was the first year in which the Department presented all five financial statements for audit, and notably the expanded scope in FY 2012 did not result in any additional qualifications. In FY 2013, the Department is actively pursuing a clean opinion on all five financial statements.

Our Financial Systems Modernization initiative remains a priority for the Department. This initiative will improve the Department's ability to provide current, accurate, and more useful financial information to DHS leaders and stakeholders through expanded business intelligence capabilities and modernizing financial systems where needed. In 2010, my office conducted extensive market research to gather and evaluate lessons learned and best practices from federal and commercial shared service providers that recently completed a financial system implementation. Our research focused on the system implementation phase in agencies across the federal sector.

We continue regular communications with these federal agencies and are working closely with the Office of Management and Budget (OMB) and the Department of the Treasury's Office of Financial Innovation and Transformation (FIT) as they formulate the governmentwide vision and roadmap for financial management systems modernization.

Thank you for your support to make DIIS efficient and effective. The Representatives who cosigned your letter will receive separate, identical responses. If we may be of further assistance, please contact Larry Bedker, Director, Financial Management, at (202) 447-(b)(6)

Sincerely,

A handwritten signature in cursive script that reads "Peggy Sherry".

Peggy Sherry  
Chief Financial Officer



SEP 26 2011



**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-11-602, Commercial Aviation: Program Aimed at High-Risk Parent Abductors Could Aid in Preventing Abductions.

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

The Honorable Peter King  
Chairman, Committee on Homeland Security

The Honorable Bennie G. Thompson  
Ranking Member, Committee on Homeland Security

The Honorable Darrell Issa  
Chairman, Committee on Oversight and Government Reform

The Honorable Elijah Cummings  
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 Jacob Lew, 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.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock".

Nelson Peacock  
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) recommendation contained in its report, GAO-11-602, Commercial Aviation: Program Aimed at High-Risk Parent Abductors Could Aid in Preventing Abductions.

**Recommendation:** Consider creating a program similar to the child abduction component of the Prevent Departure program that would apply to U.S. citizens.

**Response:** (b)(5)

(b)(5)

**SEP 26 2011**



**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-11-411, **OVERSTAY ENFORCEMENT: Additional Mechanisms for Collecting and Sharing Data Could Strengthen DHS's Efforts but Would Have Costs.**

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 Peter King  
Chairman, Committee on Homeland Security

The Honorable Bennie G. Thompson  
Ranking Member, Committee on Homeland Security

The Honorable Darrell Issa  
Chairman, Committee on Oversight and Government Reform

The Honorable Elijah Cummings  
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 Jacob Lew, 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.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock".

Nelson Peacock  
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-11-315, **OVERSTAY ENFORCEMENT: Additional Mechanisms for Collecting and Sharing Data Could Strengthen DHS's Efforts but Would Have Costs.**

GAO made five recommendations: three for U.S. Immigration and Customs Enforcement (ICE), one for U.S. Customs and Border Protection (CBP), and one recommendation for ICE, CBP, and National Protection and Programs Directorate (NPPD) collectively.

"To help ICE's execution of overstay enforcement efforts, and improve assessment of ICE programs that identify and address overstays so that program adjustments can be made, if necessary, we recommend that the Assistant Secretary of Immigration and Customs Enforcement take the following three actions:

**Recommendation 1:** "Establish a target time frame for assessing the funding and resources Enforcement and Removal Office (ERO) would require in order to assume responsibility for civil overstay enforcement and use the results of that assessment".

**Response:** DHS concurs. ICE is currently assessing the funding and resources that ERO would require in order to assume responsibility for civil overstay enforcement. ERO is currently conducting a 120 day pilot program in Los Angeles targeting non-immigrant violators. Additional information on the results of the pilot program will be forthcoming.

**Recommendation 2:** "Develop outcome-based performance measures- or proxy measures if program outcomes cannot be captured-and associated targets on Counterterrorism and Criminal Exploitation Unit's (CTCEU) progress in prevent terrorists and other criminals from exploiting the nation's immigration system."

**Response:** DHS concurs. The CTCEU has begun discussions with the National Counterterrorism Center (NCTC) to address this concern. However, the nature of "pro-active" investigations cannot be captured as a performance measure. CTCEU's approach to preventing the exploitation of the immigration system is deterrence, in that it mirrors the precept of the legal system; that compliance to the law is based on deterrence through example.

**Recommendation 3:** "Develop a performance measure for assessing the quality of leads CTCEU assigns to ICE field offices for investigations, using performance information already collected by CTCEU."

**Response:** DHS concurs. Since November 2007, the CTCEU has conducted quality reviews by sampling 1% of daily leads to correct deficient information in leads being sent to the field and to determine if additional training is needed to correct repetitive errors. The GAO noted this in the report, however, it also suggested that this metric is not sufficient in assessing the quality of overstay leads. The CTCEU disagrees with this assessment and contends that quality control reviews insure that the field agents have the most reliable information available at that time to begin an investigation. GAO correctly stated that a direct correlation could not be attributed to enforcement actions by conducting quality reviews. The success or outcome of a lead generated

by the CTCEU has many factors that cannot be accounted for by this program, such as the target moving without notification, dependence on other agencies to update their computer systems and deficiencies in collected information.

However, one of the metrics the CTCEU uses to gauge the success of this program is tracking the number of leads that are sent to the field and the results of those investigations. This review helps the CTCEU determine if continual review of policy and procedures are effective. As a result, this has led to the direct success of the totality of effort by the CTCEU in the significant increase in field arrests since FY 2007.

“To increase the completeness of exit information available for the purpose of identifying overstays, we recommend that the Commissioner of Customs and Border Protection:

**Recommendation 4:** “Analyze the costs and benefits of developing a standard mechanism for collecting I-94/I-94W forms at land POEs, and develop a standard mechanism to collect these forms to the extent that benefits outweigh the costs.”

**Response:** DHS concurs. CBP will have an independent evaluation performed of all possible solutions to the problem of developing a standard mechanism for collecting I-94/I-94W forms at land POEs, showing costs/benefits and other aspects of each solution. This evaluation, including a ranking of possible solutions, will be presented to CBP senior management for consideration.

After due consideration of the available alternatives, senior management will formulate an Action Plan for implementation by CBP to best address the development of a standard method for collection of I-94/I-94W forms at land POEs.

A report which will include the evaluation of possible solutions, the Action Plan, and a tentative schedule for implementation of the Action Plan will be completed no later than March 1, 2012.

“To improve information sharing in support of efforts to identify and take enforcement action against overstays, we recommend:

**Recommendation 5:** “The Secretary of Homeland Security direct the Commissioner of Customs and Border Protection, the Undersecretary of the National Protection and Programs Directorate, and the Assistant Secretary of Immigration and Customs Enforcement to assess the costs and benefits of creating biometric and biographic lookouts for (1) out-of-country overstays of 90 days or less who entered the country using nonimmigrant business and pleasure visas, and (2) in-country overstay leads sent to ERO and create these lookouts, to the extent that the benefits of doing so outweigh the costs.”

**Response:** DHS concurs. NPPD/US-VISIT, ICE, and CBP have met to assess the costs and benefits of creating biometric and biographic lookouts for (1) out-of-country overstays of 90 days or less who entered the country using nonimmigrant business and pleasure visas, and (2) in-country overstay leads sent to ERO.

NPPD/US-VISIT estimates that 500-600 additional lookout records would be created per year for out-of-country overstays (OCO) of 90 days or less who entered the country using



nonimmigrant business and pleasure visas. NPPD/US-VISIT estimates a 21% subsequent arrival rate, which would result in an additional 100-120 encounters per year at the ports of entry. The additional workload will be approximately one encounter every three days - nationwide. Since approximately 10,800 lookouts were created from October 2010 through June 2011, the additional 500-600 OCO lookout records would be expected to have a minimal impact on CBP operations.

The projected number of In-Country Overstay (ICO) lookout records appears substantially higher. NPPD/US-VISIT estimates that more than 15,000 ICO lookout records per year would be created. Based on a 21% subsequent arrival rate, approximately 3,150 additional encounters per year would result, or approximately 9 additional encounters per day – nationwide. The 3,150 additional encounters per year are likely a worst-case scenario. Unless these individuals depart and return to the U.S., they are not subject to CBP grounds of inadmissibility. Additionally if these individuals depart and attempt to return they would need a valid visa or a valid Electronic System for Travel Authorization (ESTA). Creation of a lookout record prevents these individuals from receiving a valid visa or approved ESTA and travelling back to the U.S.; therefore, we do not anticipate a significant adverse impact to CBP operations.

NPPD/US-VISIT would require .33 full time equivalents (FTEs) to create the additional OCO biographic and biometric lookouts at an annual cost of just over \$18,000 which NPPD/US-VISIT can absorb within current resources. Creating ICO biographic and biometric lookouts would require an additional 7 FTEs at a cost of \$386,418 annually which we cannot be absorbed within NPPD/US-VISIT current resources or funding level.

NPPD/US-VISIT will begin creating biographic and biometric lookouts for OCO of 90 days or less on July 1, 2011 assuming the minimal cost to NPPD/US-VISIT and minimal impact to CBP operations. NPPD/US-VISIT will be creating the TECS lookouts and maintaining these records, so ICE feels these will have minimal impact to Homeland Security Investigations (HSI) operations.

SEP 26 2011



**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) recommendation contained in its report, GAO-11-548R, *Mentor Protégé Programs Have Policies That Aim to Benefit Participants but Do Not Require Postagreement Tracking*.

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

The Honorable Peter T. King  
Chairman, Committee on Homeland Security

The Honorable Bennie G. Thompson  
Ranking Member, Committee on Homeland Security

The Honorable Darrell Issa  
Chairman, Committee on Oversight and Government Reform

The Honorable Elijah Cummings  
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 Jacob J. Lew, 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,

A handwritten signature in black ink, appearing to read "Nelson Peacock", with a stylized flourish at the end.

Nelson Peacock  
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) recommendation contained in its report, GAO-11-548R, *Mentor Protégé Programs Have Policies That Aim to Benefit Participants but Do Not Require Postagreement Tracking*.

**Recommendation:** To more fully evaluate the effectiveness of their mentor-protégé programs, we recommend that the OSDBU and Mentor-Protégé Program Directors of DHS, DOE, DOS, EPA, FAA, GSA, HHS, SBA, Treasury, and VA consider collecting and maintaining protégé postcompletion information.

**Response:** DHS concurs with the recommendation, and noted that it would consider following the Department of Defense model by requiring protégés to report their progress annually for 2 years after exiting the program, including providing information on annual revenue, number of employees, and participation in DHS and other government contracts. However, consistent with the GAO report recommendation, DHS stated that the potential benefits of collecting and maintaining this information would have to be weighed against potential costs.

**Actions Taken/Current Status:** DHS recognizes the benefits of collecting and maintaining protégé post completion information and will implement a post program reporting requirement beginning October 1, 2011. Protégé firms entering into the program subsequent to this date will be required to submit the information. DIIS considers the recommendation closed and will coordinate with GAO to obtain their concurrence.

JUL 18 2011



**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 Limited Official Use Only report, GAO-11-42SU, Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk.

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 Peter King  
Chairman, Committee on Homeland Security

The Honorable Bennie G. Thompson  
Ranking Member, Committee on Homeland Security

The Honorable Darrell Issa  
Chairman, Committee on Oversight and Government Reform

The Honorable Elijah Cummings  
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 Jacob Lew, 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.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock".

Nelson Peacock  
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 Limited Official Use Only report, GAO-11-42SU, Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk.

**Recommendation:** Develop, document, and implement a comprehensive annual security awareness training program for DHS headquarters that includes information on the security of wireless technologies and mobile devices.

**Response:** Office of the Chief Information Officer (OCIO) concurs. DHS Headquarters has completed and implemented an up-to-date security awareness training presentation to include information on the security of wireless technologies and mobile devices. The updated course material is attached for GAO review.

*OCIO requests closure of Recommendation #1.*

**Recommendation:** Strengthen security of the BlackBerry Enterprise Server by (1) setting "Minimum Password Length" to 8 characters or more, (2) setting "Maximum Security Timeout" to 15 minutes or less, and (3) setting "Allow Split-Pipe Connections" to "false" or document and implement compensating controls.

**Response:** (b)(7)(E)

(b)(7)(E)

(b)(7)(E) Upon approval, the form will be submitted to the Department's Information Security Office for review/signature by the DHS Chief Information Security Officer with all appropriate approvals in place by June 30, 2011.

The (b)(7)(E) setting has been implemented. The screenshots validating this correction are attached for review by GAO.

The (b)(7)(E) setting has been reviewed by the DHS Headquarters Security Team and recommendations have been made to the System Owner and Operations and Management Team for the appropriate hardening of the BlackBerry Enterprise Server. These actions are scheduled for implementation of the proposed changes to be completed by September 30, 2011.



JAN 20 2012

*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. 1101, the U.S. 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-11-873, Quadrennial Homeland Security Review: Enhanced Stakeholder Consultation and Use of Risk Information Could Strengthen Future Reviews.

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 Peter King  
Chairman, Committee on Homeland Security

The Honorable Bennie G. Thompson  
Ranking Member, Committee on Homeland Security

The Honorable Darrell Issa  
Chairman, Committee on Oversight and Government Reform

The Honorable Elijah Cummings  
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 Jacob Lew  
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.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock".

Nelson Peacock  
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-11-873, Quadrennial Homeland Security Review: Enhanced Stakeholder Consultation and Use of Risk Information Could Strengthen Future Reviews.

“To strengthen DHS’s planning, management, and execution of the next QHSR, we recommend that the DHS Assistant Secretary for Policy take the following three actions:”

**Recommendation 1:** Provide more time for consulting with stakeholders during the QHSR process to help ensure that stakeholders are provided the time needed to review QHSR documents and provide input into the review, and build this time into the department’s project planning for the next QHSR.”

**Office of Policy Update:** Concur. PLCY’s Office of Strategic Plans has begun development of the QHSR 2013 Project Plan, in coordination with MGMT’s Office of Program Analysis and Evaluation (PA&E) and other selected partners. The project plan will endeavor to incorporate increased opportunities and time for meaningful stakeholder engagement and input during the 2013 QHSR.

**Recommendation 2:** “Examine additional mechanisms for obtaining input from nonfederal stakeholders during the QHSR process, such as whether panels of state, local, and tribal government officials or components’ existing advisory or other groups could be useful, and use them for obtaining nonfederal stakeholders’ input, as appropriate, during the next QHSR.”

**Office of Policy Update:** Concur. As noted above, the 2013 QHSR Project Plan is in the early stages and planning will continue through FY2012. Throughout the project planning phase, the Department will examine the use of panels of state, local, and tribal government officials and use of existing advisory groups to obtain input. The Department will continue efforts regarding simple and accessible mechanisms that facilitate meaningful and substantive input into QHSR analysis.

**Recommendation 3:** “Examine the extent to which risk information could be used as one input to prioritize QHSR implementing mechanisms, including reviewing the extent to which the mechanisms could include characteristics, such as defined outcomes, to allow for comparisons of the risks addressed by each mechanism. To the extent that DHS determines that risk information could be used, consider such information as one input into the decision-making process for prioritizing the QHSR implementation mechanisms.”

**Office of Policy Update:** Concur. As part of its project planning, the Office of Strategic Plans intends to conduct a strategic risk assessment specific to the QHSR in advance of the next review. This assessment will then be considered, along with other factors, as an input into decision-making related to the 2013 QHSR and its implementation. The Department is committed to the continued improvement of the QHSR and looks forward to meeting the intent of GAO’s recommendations through improved project planning and precursor activities in 2012, which will in turn set the conditions for enhanced execution in 2013.





February 27, 2014

**Sent Via Email**

**Re: 2014-STFO-015**

This is the electronic acknowledgement and final response to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS) Privacy Office, dated October 21, 2013, and seeking letters from DHS to any of the following Members of Congress between 2011-2013; Representative, Michael McCaul, Rep. Candice Miller, Rep. Peter King, Rep. Patrick Meehan, Rep. Susan Brooks, Rep. Jeffrey Duncan, and Rep. Richard Hudson. While processing your request, the DHS Privacy Office located records that fall under the purview of the DHS Science and Technology Directorate (S&T). Accordingly, your request and 17 pages of responsive records were referred to S&T for processing and direct response to you. Your request was received in this office on February 4, 2014.

In a letter dated February 4, 2014, the DHS Privacy Office notified you a search of the Enterprise Correspondence Tracking System produced records responsive to your request. Of the 17 pages of responsive records referred to S&T for processing, I have determined that 17 pages of the records are releasable in their entirety, zero pages are partially releasable, and zero pages are withheld in their entirety pursuant to Title 5 U.S.C. § 552. Enclosed are the requested documents.

You have a right to appeal the above determination. Should you wish to do so, you must send your appeal and a copy of this letter, within 60 days of the date of this letter, to: Associate General Counsel (General Law), Mailstop 0655, U.S. Department of Homeland Security, Washington, DC 20528, following the procedures outlined in the DHS regulations at 6 C.F.R. § 5.9. Your envelope and letter should be marked "FOIA Appeal." Copies of the FOIA and DHS regulations are available at [www.dhs.gov/foia](http://www.dhs.gov/foia).

The Office of Government Information Services (OGIS) also mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. If you are requesting access to your own records (which is considered a Privacy Act request), you should know that OGIS does not have the authority to handle requests made under the Privacy Act of 1974. If you wish to contact OGIS, you may email them at [ogis@nara.gov](mailto:ogis@nara.gov) or call 1-877-684-6448.



Provisions of the FOIA [AND PRIVACY ACT] allow us to recover part of the cost of complying with your request. In this instance, because the cost is below the \$14 minimum, there is no charge.

If you need to contact our office again about this matter, please refer to **2014-STFO-015**. This office can be reached at [stfoia@hq.dhs.gov](mailto:stfoia@hq.dhs.gov) or (202) 254-6342.

Sincerely,

A handwritten signature in black ink, appearing to read 'Katrina Hagan', with a stylized flourish at the end.

Katrina Hagan  
FOIA Officer

Enclosures: Responsive Documents, 17 pages



# Homeland Security

July 24, 2012

The Honorable Peter T. King  
Chairman  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your June 20, 2012 letter to Secretary Napolitano concerning the Digital Imaging and Communications in Security (DICOS) standard. The Department of Homeland Security's Science and Technology Directorate (S&T) Explosives Division is working closely with the Transportation Security Administration (TSA) to create innovative solutions to security threats and challenges in the aviation sector.

S&T, in consultation with the National Electrical Manufacturers Association (NEMA), has developed a draft of DICOS Standard Version 1. Vendor testing of Version 1 is ongoing and will determine if the draft standard is sufficiently clear and comprehensive for its intended use. Upon completion of vendor testing a summary report will be provided to TSA.

DICOS Standard Version 2 is in development and is tentatively scheduled for publication later this year. This standard extends support to additional imaging modalities (e.g., Advanced Imaging Technology), updates the threat detection report format, provides requirements for data transmission and testing, as well as offers the opportunity to improve upon any issues found during DICOS Standard Version 1 testing. Furthermore, there have been preliminary discussions between S&T and TSA, in consultation with NEMA, on pursuing Version 3 of DICOS that could support cargo screening and other security missions.

S&T and TSA will continue to work together to enhance a layered aviation security approach including the development of state-of-the-art technologies, expanded use of existing and proven technology, and passenger pre-screening.

Thank you again for your interest in this matter. Representative Thompson, who co-signed your letter, will receive a separate, identical response. Should you have additional questions, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock".

Nelson Peacock  
Assistant Secretary for Legislative Affairs

October 10, 2012

The Honorable Peter T. King  
Chairman  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your recent letter to Secretary Napolitano regarding the applicability of the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act), 6 U.S.C. §§ 441-444, to technologies designed to enhance cybersecurity. The Department of Homeland Security (DHS) is committed to protecting our Nation's critical infrastructure from physical and cyber threats and believes that the SAFETY Act applies to cybersecurity technologies. As a result, DHS has extended SAFETY Act protections to three applications involving cybersecurity technologies to date. I have enclosed a description of these applications, along with examples of SAFETY Act approvals impacting the New York City metro area and the State of California.

The SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies by extending litigation and risk management systems.<sup>1</sup> The protections under these systems are triggered when the Secretary of Homeland Security determines an act to be an "act of terrorism," which is defined as "any act that the Secretary determines meets" the following requirements:

- (i) is unlawful;
- (ii) causes harm to a person, property, or entity, in the United States, or in the case of a domestic United States air carrier or a United States-flag vessel (or a vessel based principally in the United States on which United States income tax is paid and whose insurance coverage is subject to regulation in the United States), in or outside the United States; and
- (iii) uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States.

---

<sup>1</sup> SAFETY Act protections are normally granted for a period of five years and may be renewed.

Consistent with the statutory language, the Department agrees that an act need not be attributed to a specific person or entity for the act to be considered an "act of terrorism;" however, subclause (iii) includes an element of intent. The Department understands this to mean that the methods used to carry out the act provide an indication of the intent and accordingly, the Department will factor this into determining whether the act is an "act of terrorism." To date, no Secretary has invoked this provision because there has been no event where SAFETY Act Qualified Anti-Terrorism Technologies were implicated.

Thank you again for your letter and your continued support of this very important program. My staff will be in touch to arrange the briefing you requested. A separate, identical response has been sent to Chairman Lungren, who co-signed your letter. If you have any further questions, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock", with a stylized, cursive script.

Nelson Peacock  
Assistant Secretary for Legislative Affairs

Enclosure

## Approved Cybersecurity Applications

### **The Boeing Company**

April 15, 2011 - The Boeing Company provides the *Security Monitoring Infrastructure System*. The technology is a software suite that provides cyber security situational awareness and network security monitoring. This designation will expire on May 31, 2016.

### **The Boeing Company**

March 30, 2010 - The Boeing Company provides *Cyber Secure Smart Grid Integration Services* using the Secure Smart Grid Common Operating Environment. The technology is software, architecture design, and associated integration services that provide interoperability and multiple levels of cyber security to protect the Smart Grid Cyber Infrastructure. This developmental testing and evaluation designation will expire on April 30, 2013.

### **American Chemistry Council**

January 14, 2009 - The American Chemistry Council (ACC) provides the *Responsible Care Security Code*. The technology consists of a security management system encompassing 13 management practices to enhance the ability of ACC member and partner companies to deter, detect, delay, defeat, or respond to a physical or cyber attack against any form of chemical operation, whether at a fixed facility or during transportation. This designation will expire on February 28, 2014.



## **SAFETY Act Approvals impacting New York City Metro Area**

### **New York Yankees**

June 13, 2012 - New York Yankees d/b/a The New York Yankees Baseball Club provides *The New York Yankees Security Program*. The technology is a comprehensive integrated security system comprised of physical and electronic security measures, tools, and procedures designed to detect, deter, prevent, respond to, and mitigate “acts of terrorism” at Yankee Stadium. The technology includes 24/7 security coverage and incorporates systems and security practices as well as the selection and maintenance of electronic security measures. This designation and certification will expire on June 30, 2017.

### **Gold Type Business Machines, Inc.**

February 24, 2012 - Gold Type Business Machines, Inc., provides *Info-Force™*. The technology is comprised of two specialized, but complementary, software applications: Info-Cop™ and Info-Corp™. Info-Cop™ was designed to provide law enforcement officers and first responders with secure, efficient messaging, chat, resource status, controlled web access, and GPS information; as well as authorized access to real-time information from federal, state, and locally maintained and controlled databases. Info-Corp™ enables non-law enforcement public-private users to connect to Info-Cop™ servers by using the specialized software application designed for non-law enforcement users. This designation and certification will expire on March 31, 2017.

### **PricewaterhouseCoopers, LLP**

February 23, 2012 - PricewaterhouseCoopers LLP provides *Risk Management and Mitigation Planning Services*. The technology identifies risks to Critical Infrastructure and Key Resources (CIKR), measures the impact of those risks, and develops plans to mitigate the identified risks. It is used to help public and private sector clients to improve continuity of operations management. The certification currently applies only to deployments of the technology to maritime CIKR. This designation and certification will expire on March 31, 2017.

### **The Port Authority of New York and New Jersey**

December 29, 2011 - The Port Authority of New York and New Jersey provides *Articulated Precast Concrete Protective Mat System*. The technology is a system of protective mats placed on the riverbed above the Port Authority Trans-Hudson (PATH) sub-aqueous rail tunnels to protect the PATH tunnel system. This designation will expire on January 31, 2017.

### **Regal Decision Systems, Inc.**

November 4, 2011 - Regal Decision Systems, Inc. provides *Evacuation Planning Tool*. The technology provides evacuation modeling for sports stadiums through the use of a simulation model that evaluates pedestrian flow using a graphical interface which incorporates site-specific population, building specifics, and emergency management information. The technology uses algorithms for computing the evacuation planning results in both 3D animation and statistical reports for analysis. This developmental testing and evaluation designation will expire on November 30, 2014.

**Lufthansa Cargo A.G.**

July 21, 2011 - Lufthansa Cargo A.G. provides *Lufthansa Screening and Security Services*. The technology is cargo screening services that operates in conjunction with the Transportation Security Administration programs within the United States and its territories. This designation will expire on August 31, 2016.

**The Raytheon Company**

July 12, 2011 - The Raytheon Company provides the *Perimeter Intrusion Detection System*. The technology is a systems-engineering and integration service that is designed to deploy and support systems that detect, assess, track, and facilitate response to perimeter intrusions at ports, airports, sensitive buildings or other customer sites. This designation will expire on August 31, 2016.

**New York Stock Exchange-Euronext**

June 14, 2011 - New York Stock Exchange-Euronext provides the *New York Stock Exchange Security System*. The technology is comprised of command and control and integration of a multi-layered security system and services at a major financial venue. This designation will expire on June 30, 2016.

**United Technologies Corporation, UTC Fire & Security Corporation, and UTC Fire & Security Americas Corporation, Inc.**

June 7, 2011 - United Technologies Corporation, UTC Fire & Security Corporation, and UTC Fire & Security Americas Corporation, Inc., provide *MobileView*<sup>®</sup>. The technology is a mobile surveillance system consisting of digital video recorders, cameras, audio microphones, a variety of accessory and ancillary devices, and support services, which is designed for deployment on public transit vehicles such as buses, paratransit vans, and light rail and commuter rail vehicles. Also, the technology can transmit digital and audio information to a monitoring station. This designation will expire on July 31, 2016.

**Wave Dispersion Technologies, Inc.**

April 8, 2011 - Wave Dispersion Technologies, Inc., a New Jersey corporation, provides *WhisperWave*<sup>®</sup> *Small Craft Intrusion Barrier*<sup>™</sup>. The technology is a modular, rapidly deployable floating security barrier system designed to enhance maritime security by deterring, delaying, or impeding small boats traveling at high speed from approaching protected targets. Anchoring of the technology is customized for each installation and involves use of a commercially available marine-grade anchoring system, based on need. This designation will expire on May 31, 2016.

**The Port Authority of New York and New Jersey**

February 28, 2011 - The Port Authority of New York and New Jersey provides the *Protective Sleeve for Suspension Bridge Suspender Rope Damage Mitigation*. The technology is a sleeve made of steel and cementitious material designed to increase resistance of bridge suspender ropes to various threats. This designation will expire on March 31, 2016.

**Mulligan Security Corporation**

February 23, 2011 - Mulligan Security Corporation provides *Security Services*. The technology is physical security services that deter, prevent, detect, alert, and respond to a variety of security threats at high-rise commercial buildings, corporate facilities, and adjacent critical infrastructure in the New York metropolitan area, including New Jersey. This designation will expire on March 31, 2016.

## **Recent SAFETY Act Approvals impacting California**

### **Integrated Security Services, Inc**

August 20, 2012 - Integrated Security Services, Inc. provides Cargo Screening Services at Certified Cargo Screening Facilities. The technology consists of screeners and programmatic personnel for the screening of cargo in accordance with TSA's Certified Cargo Screening Program at approved Certified Cargo Screening Facilities. It includes maintaining a security plan that limits access to secure cargo screening areas, training and vetting employees in accordance with TSA guidance, adherence to all TSA specified chain-of-custody rules for this cargo, and use of TSA approved methods and/or equipment for the screening of cargo. This designation and certification will expire on September 30, 2017.

### **Harbor Offshore, Inc.**

August 3, 2012 - Harbor Offshore, Inc. provides the *Port Security Barrier (PSB) models PSB 600, PSB 5500, and PSB-T*. The technology is a seaborne barrier system that provides physical protection against high-speed boat attack and includes site assessment, installation preplanning, system installation, and maintenance training. This renewed designation will expire on August 31, 2017.

### **Hospital Shared Services**

June 20, 2012 - HSS Inc. provides *Security Services*. The technology is a suite of security services designed to secure perimeters and prevent the introduction of unauthorized persons, weapons, illicit materials, and dangerous objects into restricted areas. This renewed designation and certification will expire on July 31, 2017.

### **SAFRAN USA, Inc., Morpho Detection, Inc. and Morpho Detection International, Inc.**

February 23, 2012 - SAFRAN USA, Inc., Morpho Detection, Inc., and Morpho Detection International, Inc. provide *Integrated Logistics Support Services*. The technology is the establishment, implementation, and maintenance of an Integrated Logistics Support program to sustain Government-certified Explosives Detection Systems, Multiplexing Equipment, and associated Uninterruptible Power Supply as deployed and operated by TSA. This designation and certification will expire on March 31, 2017.

### **FirstWatch Solutions, Inc.**

February 10, 2012 - FirstWatch Solutions, Inc. provides *FirstWatch*. The technology is a real-time, web-based commercial off-the-shelf situational awareness dashboard, data surveillance, and early-warning software system that is configured to obtain reported information from existing data sources, such as safety and public health databases. Using these data, the technology performs analytics to identify trends and detect potential threats, thus allowing authorized users to securely monitor for statistically significant occurrences of reported issues that are potentially relevant to situational awareness, homeland security, and/or public health. This designation will expire on February 28, 2017.

### **Safe Environment Engineering Incorporated**

November 28, 2011 - Safe Environment Engineering Incorporated provides the *Lifeline Wireless Monitoring System*. The technology provides web-based real-time chemical, biological,

radiological, and nuclear sensor readings to Federal, State, and local decision makers and/or subject matter experts. This designation will expire on December 31, 2016.

#### **Alluviam, LLC**

June 23, 2011 - Alluviam, LLC provides HazMasterG3<sup>®</sup>. The technology is decision-support software for responding to acts of terrorism or other incidents involving chemical, biological, radiological, nuclear, and/or explosives, home-made explosives, or other hazardous materials. This renewed designation and certification will expire on July 31, 2016.

#### **Universal Protection Service**

June 3, 2011 - Universal Protection Service provides *Security and Guard Services*. The technology is physical security services for commercial buildings designed to deter, prevent, detect, alert, and respond to a variety of security threats. This includes unarmed security officers, fire/life safety, security assessments, security training, and emergency preparedness services and the recruitment, vetting, hiring, and training of its personnel which perform these services. This designation and certification will expire on January 31, 2015.

#### **FirstLine Transportation Security, Inc.**

April 1, 2011 - FirstLine Transportation Security, Inc. provides *Airline Passenger and Baggage Screening Services*. The technology consists of the provision of trained and skilled personnel to operate screening equipment, conduct pre-board passenger screening, and carry-on and checked luggage and accessible property screening to prevent prohibited items from entering the sterile area of an airport. This designation and certification will expire on May 31, 2015.

#### **The Boeing Company**

February 17, 2011 - The Boeing Company provides *Boeing's Virtual Port – Situational Awareness Systems* for Maritime Domain Applications in Support of the Port of Long Beach. The technology interfaces with third-party systems to provide geo-spatial and domain awareness in a Common Operating Picture by combining real-time data feeds and Geographic Information Systems information for the port and surrounding areas. This developmental testing and evaluation designation will expire on February 28, 2014.





Homeland  
Security

November 7, 2012

The Honorable Peter T. King  
Chairman  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman King:

Thank you for your recent letter to Secretary Napolitano regarding actions within the Department of Homeland Security (DHS) to defeat the use of radio-controlled improvised explosive devices (RCIEDs) in the United States.

DHS has ongoing efforts to assist the Department of Justice (DOJ), specifically the Federal Bureau of Investigation (FBI), in developing an electronic countermeasures (ECM) capability for federal, state, and local public safety bomb squads (PSBS). These efforts include: significant leadership by DHS and extensive collaboration with PSBS and our interagency partners, especially the FBI and Department of Defense (DOD); a rapid, initial rollout of ECM capability to PSBSs; and development of an actionable, cost-effective interagency plan to enhance and sustain ECM as an enduring capability into the future.

DHS began working with PSBSs in their efforts to obtain and employ ECM in 2005. DHS's Science & Technology Directorate (S&T) provided approximately \$2.1 million across fiscal years (FY) 2005 and 2006 to an interagency effort with DOJ and DOD that funded the development and deployment of the first generation domestic ECM system called Chameleon. This funding included compatibility testing, software load set creation, training, vehicle modification, and other development costs. Ultimately, PSBSs in 11 high-risk Urban Area Security Initiative cities were trained and equipped with Chameleon in 2006.

The Office of Infrastructure Protection's Office for Bombing Prevention subsequently led reviews of domestic counter-IED efforts mandated in both the Senate and Conference Reports accompanying the FY 2007 *Homeland Security Appropriations Act*<sup>1</sup> and in Homeland Security

---

<sup>1</sup> The Senate and Conference Reports accompanying the FY 2007 *Homeland Security Appropriations Act* directed the Secretary of Homeland Security "to develop a national strategy for bombing prevention, including a review of existing Federal, State, and local efforts in this effort" (House Report 109-699).

Presidential Directive -19, Combating Terrorist Use of Explosives in the United States (HSPD-19). The HSPD-19 report to the President, delivered to Congress in January 2008, illuminated RCIED and ECM issues at the policy level. The Office of Science and Technology Policy (OSTP) Domestic IED Subcommittee, jointly chaired by DHS S&T, OSTP, DOD, and the Joint Program Office for Countering IEDs (JPO C-IED), concurrently identified ECM research, development, testing, and evaluation as a key counter-IED technology priority. The National Bomb Squad Commanders Advisory Board (NBSCAB) was a proactive participant.

DHS worked closely with the FBI and DOD from 2007-2009 to develop implementation actions for domestic ECM requirements. The HSPD-19 implementation plan tasked DOJ, through the FBI, to lead the development of an “enhanced ECM program,” with DHS and DOD as supporting partners. To that end, in FY 2009 through FY 2011, S&T contributed an additional \$1.1 million to facilitate additional compatibility testing and vehicle modifications. In FY 2009 through FY 2011, \$1 million was provided to support transition to the next generation ECM system, including development of technical specifications and candidate systems’ compatibility testing. That process is ongoing.

At the operational level, the actual concept and fielding plan for domestic ECM must address several interrelated, highly complex, and competing challenges. More than just “bureaucratic and regulatory obstacles;” legitimate legal, technological, national security, and operational trade-offs exist that fundamentally scope the best ways and means to support PSBSs’ use of ECM in major urban areas across the United States. For example, classified information security, system licensing, and wireless interference considerations – which are much different in domestic applications than they are when ECM are used in Iraq and Afghanistan – must be carefully considered.

DHS, FBI, DOD, the Department of Commerce’s National Telecommunications and Information Agency, the Federal Aviation Administration, and NBSCAB worked together to reconcile the issues using a whole-of-government approach that unified ECM expertise and capabilities. A portion of S&T’s funding was also used to facilitate biannual, FBI-led ECM Steering Group meetings, whose stewardship of the technical and fielding issues ultimately resulted in the deployment of a domestic ECM capability, as well as a cost-effective, long-term domestic ECM model.

The interagency JPO C-IED, led by the FBI with DHS as deputy, through the ECM Steering Group, developed the enhanced National ECM Program plan in accordance with national counter-IED policy in 2012. The proposed National ECM Program would offer a cost-effective combination of military technology transfer, joint technology acquisition, and a joint federal, state, and local fielding model to sustain and enhance domestic ECM capability. This plan includes the equipment certified as effective by DHS S&T under the Support Anti-terrorism by Fostering Effective Technologies Act (SAFETY) of 2002. The updated model is based on the philosophy that a whole-of-government ECM program will provide the best capability and financial value. It posits that technology transfer using excess DOD ECM

---

inventory or surplus equipment, appropriately modified for the domestic environment, is the ideal acquisition methodology.

Despite the significant interagency efforts to date, a lack of adequate resources remains an impediment to enhancing domestic ECM capabilities through the National ECM Program. Per national counter-IED policy, DHS is a partner agency, not the lead. As such, the Department is not funded to lead this effort. However, DHS remains committed to its important but supporting role in ECM capability enhancement for PSBSs and to working with the FBI, DOD, and Congress to achieve that goal.

We recognize that the Committee may seek additional details about how the National ECM Program is meeting national counter-IED policy goals for enhancing ECM capability. Due to growing interest in domestic ECM capabilities and the inherent security sensitivities associated with ECM technology and its operational use, DHS believes it would be most appropriate moving forward to inform the Committee of additional details in a classified setting with its FBI and DOD partners.

I appreciate your interest in the Department of Homeland Security, and I look forward to continuing to work closely with you on homeland security issues. An identical response will be sent to Chairman Lungren. Should you need additional assistance, please contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock", written in a cursive style.

Nelson Peacock  
Assistant Secretary for Legislative Affairs

cc: Robert Blecksmith, Assistant Director, Federal Bureau of Investigation



**Homeland  
Security**

August 12, 2013

The Honorable Peter T. King  
Chairman  
Subcommittee on Counterterrorism  
and Intelligence  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your recent letter to Secretary Napolitano regarding fire standpipe vulnerabilities. At the Department of Homeland Security (DHS), we share your concerns regarding terrorist groups compromising the ability of our first responders to effectively respond to an attack. DHS's Science and Technology Directorate (S&T) has several programs to address terrorists' use of explosives, fire, and other means in attacks on the Nation's critical infrastructure. Efforts include vulnerability analysis, risk assessment, and mitigation design and testing for high value buildings and other structures such as tunnels and bridges. For example, the S&T-developed Integrated Rapid Visual Screening Tool, which has been widely adopted in New York and elsewhere, rapidly and systematically quantifies the risk and resilience of buildings to manmade and selected natural hazards capable of causing catastrophic losses in terms of fatalities, injuries, damages or interruption.

While S&T's efforts do not focus on the specific vulnerability or possible protective countermeasures associated with fire standpipes at this time, we have reached out to our interagency, state, and local partners to consider possible approaches to address this vulnerability. Should you need additional assistance, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in blue ink, appearing to read "Brian de Vallance".

Brian de Vallance  
Acting Assistant Secretary for Legislative Affairs

cc: Salvatore Cassano, Fire Commissioner, City of New York

AUG 05 2011



**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-11-606, "NATIONAL PREPAREDNESS: DHS and HHS Can Further Strengthen Coordination for Chemical, Biological, Radiological, and Nuclear Risk Assessments"

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 Peter King  
Chairman, Committee on Homeland Security

The Honorable Bennie G. Thompson  
Ranking Member, Committee on Homeland Security

The Honorable Darrell Issa  
Chairman, Committee on Oversight and Government Reform

The Honorable Elijah Cummings  
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 Jacob Lew, 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.

Respectfully,

A handwritten signature in black ink, appearing to read "Nelson Peacock".

Nelson Peacock  
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-11-606, "NATIONAL PREPAREDNESS: DHS and HHS Can Further Strengthen Coordination for Chemical, Biological, Radiological, and Nuclear Risk Assessments"

"To ensure that DHS senior officials are able to monitor progress on the development of the proposed strategic and implementation plans for DHS's CBRN risk assessment efforts, we recommend that the Secretary of Homeland Security:

**Recommendation:** develop and document interim time frames and milestones as part of a plan to develop, finalize, and obtain interagency agreement on the written procedures for interagency development of the TRAs and MTAs that DHS intends to issue as strategic and implementation plans."

**Response:** The DHS Science and Technology Directorate (S&T) has held multiple meetings with members of the Department of Health and Human Services (HHS) and has been working diligently on an implementation strategy for conducting and issuing material threat determinations. The draft implementation strategy is almost ready for circulation and updates for finalization. The goal is to have the implementation strategy completed by the end of calendar year 2011. With regard to the terrorist risk assessments (TRAs), S&T has already begun developing a Strategic Implementation Plan. The draft Strategic Implementation Plan will be completed by the end of FY 2011 and will be distributed to HHS for review, comment, and suggestions for improvement. The goal is to have an agreed upon Strategic Implementation Plan no later than June 2012.

July 21, 2011



**Homeland  
Security**

The Honorable Michael McCaul  
Chairman, Subcommittee on Oversight, Investigations,  
and Management  
U.S. House of Representatives  
Washington D.C. 20515

Dear Mr. Chairman:

On Friday July 15, 2011, we testified before the committee and due to time constraints, many concerns raised in the opening statements were not able to be addressed. We wanted to take this opportunity to share with you the progress that has been and continues to be made with regard to leveraging technology and the Department's programs in securing the border, and to correct the reported errors regarding the Department's Advanced Spectroscopic Portal (ASP) program.

As was stated in the hearing, DHS is highly focused on leveraging research and development investments made by the federal government, the commercial sector or universities. As part of its recent organizational realignment, the Science and Technology Directorate created the Research and Development Partnerships Group, which reports directly to the Under Secretary, to focus our "technology foraging" efforts. As an example of our many interactions with DoD, Under Secretary of Defense for Acquisition, Technology, and Logistics Dr. Ashton Carter, DHS Under Secretary for S&T Dr. Tara O'Toole and DHS Under Secretary for Management Rafael Borras meet quarterly under the Capability Development Working Group. This group explores capabilities of mutual departmental interest, decides on appropriate implementation paths that avoid duplication of effort, and informs policy, planning, and decision making. Under Secretary O'Toole also co-chairs the White House Office of Science and Technology Policy's Committee on Homeland and National Security with Assistant Secretary of Defense for Research and Engineering Zachary Lemnios. The committee and its subcommittees, consisting of agencies across the federal government, collaboratively develop executable research and development plans.

It is critical in these efforts, however, that the existing technologies line up with DHS's operational requirements. Part of the problem with past acquisitions has been the attempt to insert off-the-shelf technologies, designed for different missions, in to DHS programs without a careful comparison to DHS's specific operational needs. The shared focus of the Under Secretary for Management, the Under Secretary for Science and Technology, and Secretary Napolitano on leveraging S&T in the "front end" of acquisition is targeted specifically at ensuring that DHS either selects the proper off-the-shelf technology when it exists, or receives the technology through a disciplined research, development, and acquisition process.

As you correctly noted in the hearing, the Secure Border Initiative was started in 2006. This was before the current management controls were put in place, specifically Acquisition Management

Directive 102-01. Directive 102-01 was signed by then Under Secretary Elaine Duke in January of 2010. In July of 2010, the troubled SBInet program was directed to present a revised Analysis of Alternatives (AoA) in accordance with Directive 102-01 that reexamined the operator's needs. This rigorous analysis and mandatory engagement with the field operations resulted in a much more rational technology plan that includes proven elements of the former SBInet program while better utilizing off-the-shelf solutions. Through our management controls, we directed the suspension of SBInet, forced a replan of border security technology, and supported a new plan to increase operational coverage and provide deployment flexibility that was not present in the prior program plan.

Regarding the recent *Washington Post* article, we want to point out some key items that the newspaper story did not cover. First, Advanced Spectroscopic Portal monitors, or ASPs, have been tested and subject to review and evaluation for over three years. These test data were used to inform a decision on whether to go forward with acquisition and deployment activities. In April of 2011 the Department held an Acquisition Review Board (ARB) on ASPs. The ARB directed the Domestic Nuclear Detection Office (DNDO) and Customs and Border Protection (CBP) to pursue a revised program that address limitations in cargo conveyance scanning technologies based on the Model-Test-Model approach recommended by the National Academies of Science. This revised program was directed by the ARB to include commercially-developed systems and an analysis of alternatives. Finally, the most recent ASP contract expired on July 11<sup>th</sup> of this year – there is no more existing contract to purchase radiation monitors today, nor will there be until such time that a new set of requirements is developed by DNDO and CBP, and approved by the Department's ARB.

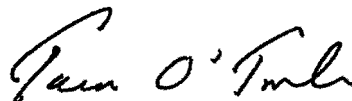
We acknowledge that many of the Department's legacy programs have faced challenges that both the Office of the Inspector General (OIG) and the Government Accountability Office (GAO) have repeatedly commented on; however, even the OIG noted in its recent June report (OIG-11-91) that significant progress has been made in maturing the Department's acquisition process and program management capabilities. In fact, the report notes that the Department has implemented all five recommendations to enhance oversight, established and strengthened the Department's Acquisition Program Management Division, and addressed procurement staff shortages and staff authority.

We thank you for your support of the Department of Homeland Security, and an identical letter has been sent to Ranking Member Keating. If we can be of any future assistance, please contact us at (202) 447-3400 or (202) 254-6033.

Sincerely,



Rafael Borrás  
Under Secretary for Management



Tara O'Toole, M.D., M.P.H.  
Under Secretary for Science & Technology





Homeland  
Security

April 17, 2014

SENT VIA EMAIL

Re: **2014-IAFO-0059**

This is the final response to your Freedom of Information Act (FOIA) request to the Department of Homeland (DHS), dated April 20, 2013. Responsive documents for your request were subsequently forwarded to and received by the Office of Intelligence and Analysis (I&A) on February 4, 2014. You are seeking "a copy of each written response or letter from the Department of Homeland Security to a Congressional committee (not a congressional office) (or Committee Chair) in calendar years 2012 and 2013 to date. By this, you mean one-time type responses to Committee inquiries, excluding from the scope of this request regular periodic reports and constituent responses to a congressional office. In your September 30, 2013 email to this office, you agreed to a copy of each written response or letter from the Department of Homeland Security to any of the following Members of Congress in calendar years 2011, 2012 and 2013 to date: Rep. Michael McCaul, Rep. Candice Miller, Rep. Peter King, Rep. Patrick Meehan, Rep. Susan Brooks, Rep. Jeffrey Duncan, and Rep. Richard Hudson.

DHS provided 1 page of documentation that was determined to belong to I&A. Upon review of that document, I&A discovered the enclosure of 5 pages associated with the letter and is providing you a copy of those as well.

Based on the review of these documents, I&A is providing the following:

2 page(s) are released in full (RIF)  
4 page(s) are released in part (RIP)

The exemptions cited for withholding records or portions of records are marked below.

Freedom of Information Act, 5 U.S.C. § 552			Privacy Act, 5 U.S.C. § 552a
<input type="checkbox"/> 552(b)(1)	<input type="checkbox"/> 552(b)(5)	<input type="checkbox"/> 552(b)(7)(C)	<input type="checkbox"/> 552a(j)(2)
<input type="checkbox"/> 552(b)(2)	<input checked="" type="checkbox"/> 552(b)(6)	<input type="checkbox"/> 552(b)(7)(D)	<input type="checkbox"/> 552a(k)(2)
<input checked="" type="checkbox"/> 552(b)(3)	<input type="checkbox"/> 552(b)(7)(A)	<input checked="" type="checkbox"/> 552(b)(7)(E)	<input type="checkbox"/> 552a(k)(5)



<input type="checkbox"/> 552(b)(4)	<input type="checkbox"/> 552(b)(7)(B)	<input type="checkbox"/> 552(b)(7)(F)	<input type="checkbox"/> Other:
------------------------------------	---------------------------------------	---------------------------------------	---------------------------------

### **Exemption 3, 5 U.S.C. § 552(b)(3)**

Exemption 3 protects “information specifically exempted from disclosure by [another] statute.” *See* 5 U.S.C. § 552 (b)(3). In this instance 50 U.S.C. § 3024(i) and 6 U.S.C. § 121(d)(11) exempts information regarding intelligence sources and methods from unauthorized disclosure. I&A is withholding information which would lead to the revelation of intelligence sources and methods.

### **Exemption 6, 5 U.S.C. § 552(b)(6)**

Exemption 6 exempts from disclosure personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a balancing of the public’s right to disclosure against the individual’s right privacy. The types of documents and/or information that we have withheld may consist of names. The privacy interests of the individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

### **Exemption 7(E), 5 U.S.C. § 552(b)(7)(E)**

Exemption 7(E) protects all law enforcement information that “would disclose techniques and procedures for law enforcement investigation or prosecution, or would disclose guidelines for law enforcement investigations or prosecution if such disclosure could reasonably be expected to risk circumvention of the law.” *See* 5 U.S.C. § 552(b)(7)(E). DHS-I&A is withholding from disclosure specific information which could reasonably be expected to risk circumvention of the law.

You have a right to appeal this response.<sup>1</sup> Should you wish to do so, you must send your appeal and a copy of this letter, within 60 days of the date of this letter, to: Associate General Counsel (General Law), U.S. Department of Homeland Security, Washington, D.C. 20528, following the procedures outlined in the DHS regulations at 6 C.F.R. § 5.9. Your envelope and letter should be marked “FOIA Appeal.” Copies of the FOIA and DHS regulations are available at [www.dhs.gov/foia](http://www.dhs.gov/foia).

The Office of Government Information Services (OGIS) also mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. If you wish to contact OGIS, you may email that entity at [ogis@nara.gov](mailto:ogis@nara.gov) or call 877-684-6448.

---

<sup>1</sup> For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. *See* 5 U.S.C. 552(c) (2006 & Supp. IV 2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

If you need to contact our office concerning this request, please call 202-447-4883 and refer to **2014-IAFO-0059**.

Sincerely,

A handwritten signature in cursive script that reads "Priscilla Waters".

Priscilla Waters  
Intelligence and Analysis  
FOIA Officer

Enclosures:

1. Letter from Rep. Meehan
2. Response to Questions from Congressman Patrick Meehan and Congresswoman Jackie Speier



Homeland  
Security

February 13, 2012

The Honorable Patrick Meehan  
U.S. House of Representatives  
Washington, DC 20515

Dear Representative Meehan:

Thank you for your letter requesting additional information on the Department of Homeland Security's (DHS) guidelines on the use of social media for intelligence purposes. Appropriately gathering information from social media and other publicly available forums, while respecting privacy and civil liberties, is an important part of the DHS Office of Intelligence and Analysis's mission. While social media provides only one aspect of open source intelligence, the collection activities performed by the cadre of open source collection professionals within our Open Source Enterprise receive thorough training as well as comprehensive oversight from both our DHS legal and intelligence oversight staffs.

Please find the enclosed responses to your specific questions. We look forward to working with you on this and other homeland security matters. Should you need additional assistance, please do not hesitate to contact me through the DHS Office of Legislative Affairs at (202) (b) (6)

Sincerely,

A handwritten signature in black ink, appearing to read "Caryn A. Wagner".

Caryn A. Wagner  
Under Secretary for Intelligence and Analysis

Enclosure

**Response to Questions from Congressman Patrick Meehan and Congresswoman Jackie Speier**

1. *When will the guidelines on the use of social media for intelligence purposes be issued to the Department? Prior to this new set of guidelines, what previous guidelines were intelligence analysts operating under when monitoring social media websites? Who are the principle DHS officials involved in the drafting of this guidance? Will there be one uniform set of guidelines Department-wide, or will the guidelines only be applicable to the DHS Intelligence Enterprise or DHS members of the Intelligence Community? If and/or when they are available, please provide copies of all pertinent, current, written guidelines to the Subcommittee.*

The Office of Intelligence and Analysis (I&A) is currently participating in an Office of the Director of National Intelligence (ODNI)-led interagency working group to develop an integrated approach to social media. The Department of Homeland Security's (DHS) role in this effort is to ensure homeland security requirements and equities are adequately represented, while ensuring the protection of the privacy and civil rights and civil liberties of U.S. Persons (USPERs). No specific timetables have been set regarding any Intelligence Community (IC) social media guidelines.

I&A is restricted to the collection of information overtly or from publicly available sources, in accordance with *Executive Order (EO) 12333*, as amended, and the DHS I&A policy dated April 3, 2008, *Interim Intelligence Oversight (IO) Procedures for the Office of Intelligence and Analysis*. In addition, the collection of open source information, like the collection of all publicly available information, must conform to the ODNI's *Civil Liberties and Privacy Guidance for Intelligence Community Professionals: Properly Obtaining and Using Publicly Available Information*. Within I&A, the Division most directly engaged in the use of social media is the Collection Requirements Division, which operates the Open Source Enterprise (OSE). The OSE collects, acquires, processes, stores, and disseminates raw open source information and open source intelligence (OSINT), to include publicly available information, in support of the full array of DHS missions. Collection is based on articulated requirements from I&A or other IC analysts that are consistent with I&A missions and approved collection categories.

Separate from the I&A OSE, the DHS Office of Operations Coordination and Planning maintains a media monitoring capability for publicly available information within the DHS National Operations Center (NOC). Section 515 of the Homeland Security Act, as amended, established the NOC as the principal operations center for the Department, responsible for providing situational awareness and a common operating picture to the entire federal government and state, local, and tribal governments, as appropriate, in the event of a natural disaster or terrorist act; and for ensuring critical terrorism and disaster related information reaches government decision makers. The NOC's media monitoring capability contributes to this statutory mission by utilizing publicly available information and search tools to identify breaking or evolving events.

The Department is also developing a Management Directive for Privacy Protections in Operational Use of Social Media. The Management Directive will be enforceable throughout the Department, and will identify the authorities, restrictions, and privacy oversight related to use of social media for operational purposes. The Management Directive will also provide instructions on how to embed privacy protections into the operational use of social media and each investigation performed by Department personnel.

2. *How will the guidelines take privacy and civil liberties of U.S. persons into account? Have there been any Privacy Impact Assessments or other assessments conducted on the collection of information from social media sites? If so, please provide the Subcommittee with copies of the assessments.*

DHS I&A policy dated April 3, 2008, *Interim Intelligence Oversight (IO) Procedures for the Office of Intelligence and Analysis* provides guidance on the procedures governing the collection, retention, and dissemination of USPER information by I&A, including USPER information collected by the I&A OSE (a copy of this memo is provided). DHS I&A must also follow the rules outlined in its Privacy Act System of Records Notice (SORN), DHS/I&A-001, for collection on USPERs. In addition to this guidance, the DHS Privacy Office is currently working with I&A to produce a Privacy Impact Assessment (PIA) for the I&A OSE.

The NOC partnered with the DHS Privacy Office in 2009 to ensure that its media monitoring capability would be established with the necessary privacy protections. In 2010, the NOC, in coordination with the DHS Privacy Office, began a media monitoring initiative to assist DHS and its Components involved in the Haiti earthquake response. This was followed by two additional media monitoring initiatives, the 2010 Winter Olympics in Vancouver, British Columbia and the response to the April 2010 Deep Water Horizon Gulf Coast oil spill. Following the three discrete social media monitoring pilots by the NOC, the Privacy Office did a thorough (and public) Privacy Compliance Review of the NOC's implementation of the PIAs' privacy protections. The Privacy Office's review found that the NOC's social media monitoring activities did not collect PII, did not monitor or track individuals' comments, and complied with the stated privacy parameters set forth in the underlying PIAs.

Given the positive assessment of the three pilots, OPS and the Privacy Office designed a holistic set of privacy protections to be implemented whenever information made available through social media is being reviewed for situational awareness and establishing a common operating picture. In June 2010, the Department released its *Publicly Available Social Media Monitoring and Situational Awareness Initiative* PIA, incorporating these protections. This PIA describes how the NOC uses Internet-based platforms that provide a variety of ways to review information accessible on publicly-available online fora, blogs, public websites, and message boards. Through the use of publicly-available search engines and content aggregators, the NOC reviews information accessible on certain heavily-trafficked social media sites for information that the NOC can use to provide situational awareness and establish a common operating picture.



After conducting a second Privacy Compliance Review, the Privacy Office determined that the June 2010 PIA should be updated to allow for the collection and dissemination of PII in a very limited number of situations in order to respond to the evolving operational needs of the NOC. DHS issued a publicly available PIA Update and publicly available Social Media Monitoring and Situational Awareness Initiative SORN on January 6, 2011 and February 1, 2011. In November 2011, the Privacy Office found the NOC to be in compliance with the privacy parameters set forth in the January 6, 2011 PIA update and the February 1, 2011 SORN. All privacy documents referenced in this paragraph are available to the public through [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

3. *What technologies does DHS leverage to ingest the massive amount of data from the Internet to analyze broad trends? Does DHS need more research and development in this area?*

Members of the I&A OSE collect and report Open Source information related to specific DHS or IC intelligence requirements (e.g., information of intelligence value posted to a social media or blog site associated with a known violent extremist, or information from open press concerning a DHS mission area, such as developments in human trafficking). The I&A OSE only employs internet tools that are “in the general public use,” and does not employ specialized tools to ingest large amounts of data from the public sphere. As the use of social media and its potential contribution to intelligence development is a relatively new field for the IC, additional research and development (R&D) will certainly benefit our understanding of how to best and appropriately use social media as an intelligence tool. Currently, I&A leverages R&D conducted by IC partners, such as that being done at the ODNI’s Open Source Center (OSC).

The NOC uses publicly available search engines and content aggregators to follow publicly posted and available information.

4. *Is there a strategic plan for expanding or evolving the DHS Open Source Enterprise to better take advantage of social media? Do you anticipate a larger budget request in this area for FY 2013? How many analysts are currently dedicated to open source intelligence collection and analysis? Please state how many of these analysts are government employees and how many are contractors.*

I&A produced an Open Source Strategic Vision in 2008, which is undergoing revision and will be aligned with the ODNI’s interagency social media initiative. Future resource levels will be driven by requirements; however there are no immediate plans for expanding the OSE program.


Currently, I&A OSE employs (b) (7)(E), (b) (3) full time equivalents to conduct open source collection and raw reporting, dissemination, and library services. While the I&A OSE personnel are uniquely dedicated to open source, other I&A personnel may conduct research using open sources to contribute to their analytic production, as needed.

5. *When conducting open source intelligence training for DHS and state and local fusion center analysts, is there guidance specific to social media included in the program?*

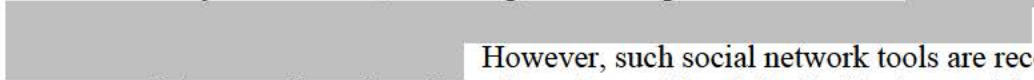
I&A conducts an Open Source Practitioners Course (OSPC) for DHS employees as well as federal and state, local, tribal, and territorial partners to assist them in understanding the open source landscape, conducting open source research, assessing the utility of open source tools, and using various consolidated research resources. The course includes training on search engine tools, including social media networking. The instruction also continually underscores the limitations imposed by 28 *Code of Federal Regulations Part 23, Criminal Intelligence Systems Operating Policies*. The training stresses the importance of consulting the appropriate General Counsel, privacy, or civil rights and civil liberties department for further guidance. All 76 fusion centers have an approved privacy policy that is at least as comprehensive as the *Information Sharing Environment Privacy and Civil Rights and Civil Liberties Guidelines*.

6. *How does DHS ensure specialized training for social media analysis? For example, as you know, traditional sources of intelligence such as human intelligence (HUMINT) are vetted to determine source credibility and reliability over a period of time. Social media lends itself to a great deal of misinformation and disinformation, both of which significantly impacts the end product if not correctly identified. How will DHS ensure that its analysts are fully equipped to handle this task?*


I&A's OSPC provides training on search engine tools, including social media networking. (b) (7)(E), (b) (3)



I&A recognizes that the ability of individuals to mask their identity on the Internet has made credibility assessments, or vetting, more complex and difficult. (b) (7)(E), (b) (3)



However, such social network tools are recognized as vanguards in reporting crises throughout the world and for facilitating social movements. As the use and practice of adopting open source information into IC analytical products matures, I&A will incorporate appropriate techniques into the OSINT and analytic training and education regimens. (b) (7)(E), (b) (3)





(b) (7)(E)

7. *What are the authorities and restrictions for the DHS Open Source Enterprise collection activities? Do you believe any new authorities are necessary to enhance this mission?*

As mentioned above, I&A collects intelligence and information overtly or from publicly available sources, in accordance with 6 USC 121; EO 12333, as amended; and I&A's April 3, 2008 IO procedures. In addition, the I&A OSE follows IC Directive 301, National Open Source Enterprise, July 11, 2006, and the ODNI Civil Liberties and Privacy Guidance for IC Professionals: Properly Obtaining and Using Publicly Available Information, July 2011. In addition, DHS I&A's collection activities for USPERs are covered by DHS/I&A-001 Enterprise Records System, published on May 15, 2008 at 73 FR 28128. This includes collection from social media. I&A has sufficient authority to conduct its Open Source mission.

8. *What is the relationship between the DHS Open Source Enterprise and the Office of the Director of National Intelligence's Open Source Center (OSC)? Does DHS leverage OSC materials, and are DHS open source products available at the OSC?*

The I&A OSE and the ODNI's OSC operate under different authorities and procedures. The I&A OSE and the OSC, however, interact on a variety of levels that span training, collections, and analysis. Both elements are represented on the ODNI's National Open Source Committee and its subcommittees. The I&A OSE takes advantage of the OSC Open Source Academy (OSA) for training and reciprocates by providing blocks of education on the I&A OSE and domestic collection at OSA courses. The I&A OSE and the OSC have a working relationship in areas of mutual interest like terrorism and international trafficking and smuggling. (b) (7)(E), (b) (3)

DHS all-source analytical efforts leverage OSC reporting for DHS analytic products. I&A OSE raw reporting, in the form of Open Source Information Reports, is available to the wider IC, including the OSC.



Transportation  
Security  
Administration

April 14, 2015

**3600.1**

Case Number: 2014-TSFO-00197

This letter responds to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS) dated April 20, 2013, and revised on September 30, 2013, for "a copy of each written response or letter from the Department of Homeland Security to any of the following Members of Congress in calendar years 2011, 2012 and 2013 to date: Rep. Michael McCaul, Rep. Candice Miller, Rep. Peter King, Rep. Patrick Meehan, Rep. Susan Brooks, Rep. Jeffrey Duncan, and Rep. Richard Hudson." By letter dated February 4, 2014, you were advised by DHS that some of the responsive records were being transferred to the Transportation Security Administration (TSA) for review and direct response to you.

TSA has completed its review and identified certain materials that will be released to you. Portions not released are being withheld pursuant to the Freedom of Information Act, 5 U.S.C. § 552. Please refer to the Applicable Exemptions list at the end of this letter that identifies the authority for withholding the exempt material, which is indicated by a mark appearing in the block next to the exemption. An additional enclosure with this letter explains these exemptions in more detail.

Fourteen pages of records were incorrectly referred to the TSA and should have been referred to the U.S. Customs and Border Protection (CBP). We will forward these pages to them for review and direct response to you. Contact information to CBP is:

U.S. Customs and Border Protection  
Attn: FOIA Officer Sabrina Burroughs  
1300 Pennsylvania Ave., NW, Mint Annex  
Washington, D.C. 20229-1181  
Telephone at 202-325-0150

The rules and regulations of the TSA applicable to Freedom of Information Act requests are contained in the Code of Federal Regulations, Title 6, Part 5. They are published in the Federal Register and are available for inspection by the public.

### Fees

There are no fees associated with processing this request because the fees incurred do not exceed the minimum threshold necessary for charge.

### Administrative Appeal

In the event that you wish to appeal this determination, an administrative appeal may be made in writing to Kimberly Walton, Assistant Administrator, Office of Civil Rights & Liberties, Ombudsman and Traveler Engagement (CRL/OTE), Transportation Security Administration, 601 South 12<sup>th</sup> Street, East Building, E7-121S, Arlington, VA 20598-6033. Your appeal **must be submitted within 60 days** from the date of this determination. It should contain your FOIA request number and, to the extent possible, the reasons why you believe the initial determination should be reversed. In addition, the envelope in which the appeal is mailed should be prominently marked "FOIA Appeal." Please note that the Assistant Administrator's determination of the appeal will be administratively final.

If you have any questions pertaining to your request, please feel free to contact the FOIA Branch at 1-866-364-2872 or locally at 571-227-2300.

Sincerely,



Angela Washington  
Acting FOIA Officer

#### Summary:

Number of Pages Released in Part or in Full: 14

Number of Pages Withheld in Full: 0

Number of Pages Referred: 12

### **APPLICABLE EXEMPTIONS FREEDOM OF INFORMATION ACT AND/OR PRIVACY ACT**

#### **Freedom of Information Act (5 U.S.C. 552)**

☐ (b)(1) ☐ (b)(2) ☐ (b)(3) ☐ (b)(4) ☐ (b)(5) ☒ (b)(6)

☐ (b)(7)(A) ☐ (b)(7)(B) ☐ (b)(7)(C) ☐ (b)(7)(D) ☐ (b)(7)(E) ☐ (b)(7)(F)

Enclosures



FREEDOM OF INFORMATION ACT  
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

Transportation Security Administration (TSA) FOIA Branch applies FOIA exemptions to protect:

Exemptions

**Exemption (b)(1):** Records that contain information that is classified for national security purposes.

**Exemption (b)(2):** Records that are related solely to the internal personnel rules and practices of an agency.

**Exemption (b)(3):** Records specifically exempted from disclosure by Title 49 U.S.C. Section 114(r), which exempts from disclosure Sensitive Security Information (SSI) that “would be detrimental to the security of transportation” if disclosed.

**Exemption (b)(4):** Records that contain trade secrets and commercial or financial information obtained from a person that is privileged or confidential.

**Exemption (b)(5):** Inter- or intra-agency records that are normally privileged in the civil discovery context. The three most frequently invoked privileges are the deliberative process privilege, the attorney work-product privilege, and the attorney-client privilege:

- Deliberative process privilege – Under the deliberative process privilege, disclosure of these records would injure the quality of future agency decisions by discouraging the open and frank policy discussions between subordinates and superiors.
- Attorney work-product privilege – Records prepared by or at the direction of a TSA attorney.
- Attorney-client privilege – Records of communications between an attorney and his/her client relating to a matter for which the client has sought legal advice, as well as facts divulged by client to attorney and any opinions given by attorney based on these.

**Exemption (b)(6):** Records that contain identifying information that applies to a particular individual when the disclosure of such information “would constitute a clearly unwarranted invasion of personal privacy.” This requires the balancing of the public’s right to disclosure against the individual’s right to privacy.

**Exemption (b)(7)(A):** Records or information compiled for law enforcement purposes, but only to the extent that production of such law enforcement records or information...could reasonably be expected to interfere with law enforcement proceedings.

**Exemption (b)(7)(C):** Records containing law enforcement information when disclosure “could reasonably be expected to constitute an unwarranted invasion of personal privacy” based upon the traditional recognition of strong privacy interests ordinarily appropriated in law enforcement records.

**Exemption (b)(7)(E):** Records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

**Exemption (b)(7)(F):** Records containing law enforcement information about a person, in that disclosure of information about him or her could reasonably be expected to endanger his or her life or physical safety.

PRIVACY ACT  
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

Transportation Security Administration (TSA) FOIA Branch applies Privacy Act exemptions to protect:

Exemptions

**Exemption (d)(5):** Information compiled in reasonable anticipation of civil action or proceeding; self-executing exemption.

**Exemption (j)(2):** Principal function criminal law enforcement agency records compiled during course of criminal law enforcement proceeding.

**Exemption (k)(1):** classified information under an Executive Order in the interest of national defense or foreign policy.

**Exemption (k)(2):** Non-criminal law enforcement records; criminal law enforcement records compiled by non-principal function criminal law enforcement agency; coverage is less broad where individual has been denied a right, privilege, or benefit as result of information sought.

**Exemption (k)(5):** Investigatory material used only to determine suitability, eligibility, or qualifications for federal civilian employment or access to classified information when the material comes from confidential sources.

**Exemption (k)(6):** Testing or examination material used to determine appointment or promotion of federal employees when disclosure would compromise the objectivity or fairness of the process.

Secretary

U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

February 4, 2011

The Honorable Peter T. King  
Chairman  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman King:

Thank you for your letter regarding the Transit Security Grant Program (TSGP).

The Department is currently in the process of developing fiscal year (FY) 2011 grant guidance for each of the grants it administers, including TSGP, pending a FY 2011 appropriation. As we do each year, we are working closely with stakeholders across state and local governments and the mass transit community to gather feedback on proposed options and the overall TSGP process. Based on these discussions, several options for the FY 2011 TSGP are currently under consideration. All of these proposals include keeping the Regional Transit Security Working Group's construct in place. Further, all of the proposals continue to prioritize operational deterrence activities and use a risk-based approach to target funds to those regions and systems with the highest risk, both in terms of total system/regional risk and asset-specific risk.

We will continue to keep you apprised of the options that are under consideration and look forward to working closely with you once funding is appropriated for TSGP and other homeland security grant programs. We would also be happy to brief committee staff on our current stakeholder outreach process and efforts and address any questions or concerns regarding the different options being considered for the FY 2011 TSGP. Ultimately, our goal is to design the TSGP in a manner that best serves the needs and security requirements of the mass transit community, and best protects the traveling public from evolving threats.

Thank you again for your letter. I look forward to fostering a close working relationship with you in your new role as Chairman of the House Committee on Homeland Security. Should you need additional assistance, please do not hesitate to contact me at (202) 282-8203.

Yours very truly,

A handwritten signature in black ink, appearing to read "Janet Napolitano", with a stylized flourish at the end.

Janet Napolitano

[www.dhs.gov](http://www.dhs.gov)

JAN 11 2012



**Homeland  
Security**

The Honorable Michael T. McCaul  
Chairman  
Subcommittee on Oversight, Investigations  
and Management  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman McCaul:

Thank you for your recent letter regarding the September 16, 2011 hearing on airport security and preventing future terrorist attacks. We appreciate your interest in the Screening of Passengers by Observation Techniques (SPOT) program and to our ongoing assessment of perimeter airport security throughout the United States.

*Screening of Passengers by Observation Techniques (SPOT)*

TSA currently deploys approximately 3,000 Behavior Detection Officers (BDO), all trained in SPOT, to over 160 airports nationwide. With the passage of the FY12 appropriations bill, Congress funded an additional 145 BDOs.

TSA is currently piloting a program for enhanced SPOT, which is undergoing a proof-of-concept at Boston's Logan International Airport and Detroit's Metropolitan Wayne County Airport. TSA is also working with DHS' Science & Technology Directorate (S&T) to design and conduct additional validation studies and trade-off analysis to continue to improve upon its behavior detection capability.

*Perimeter Security*

TSA continues to work to improve perimeter security at airports across the Nation to ensure that each facility is fully compliant with access control and other perimeter security requirements set forth in 49 CFR 1542. Specific perimeter security measures and enforceable requirements are established in each airport's Airport Security Program (ASP), and the airport operator, TSA Federal Security Director (FSD), and air carriers work together to produce the standards at each airport.

As part of TSA's ongoing partnerships with airport operators, TSA works closely with local airports as well as law enforcement to strengthen their security posture. In March 2011, with the support from the Homeland Security Studies and Analysis Institute and following assessments of 22 U.S. airports, TSA provided airport operators with a compendium of best practices in perimeter security and risk assessment tools. In addition, in May 2011, TSA

The Honorable Michael T. McCaul

Page 2

produced and disseminated *Recommended Design Guidelines for Airport Planning, Design, and Construction*, which provides perimeter security recommendations to airport operators on items such as fencing, building design, walls, electronic boundaries and new technologies, natural barriers, gates, doors, guard stations, vehicle inspections stations, road barriers, fence clear zones, lighting, locks, and closed-circuit television.

TSA's goal at all times is to maximize transportation security and stay ahead of evolving terrorist threats while protecting passengers' privacy, and facilitating the efficient flow of travelers and legitimate commerce. TSA's SPOT program and airport perimeter security initiatives are part of this comprehensive effort.

Thank you again for your letter. I look forward to fostering a close working relationship with you on this and other homeland security issues. Should you need further assistance, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read 'Nelson Peacock', with a stylized flourish at the end.

Nelson Peacock  
Assistant Secretary  
Office of Legislative Affairs



FEB 21 2012

U.S. Department of Homeland Security  
601 South 12th Street  
Arlington, VA 20598



**Transportation  
Security  
Administration**

The Honorable Peter T. King  
Member, U.S. House of Representatives  
Attention: Mr. Michael Schillinger  
1003 Park Boulevard  
Massapequa Park, NY 11762

Dear Congressman King:

Thank you for your letter of February 7, 2012, written on behalf of your constituent, (b)(6) regarding his concerns that he may be on a watch list after being told by Xerox Direct that they cannot accept online orders from him.

To conduct watch list matching, the Transportation Security Administration's (TSA) Secure Flight program uses subsets of the Terrorist Screening Database (TSDB), the U.S. Government's consolidated watch list compiled from information provided by U.S. intelligence and law enforcement agencies and maintained by the U.S. Terrorist Screening Center. The TSDB includes the No Fly List and the Selectee List. Individuals on the No Fly List are prohibited from traveling on commercial aircraft. Individuals on the Selectee List are permitted to fly but receive secondary screening at airport security checkpoints prior to boarding.

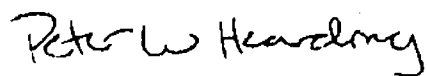
For more information on the Terrorist Screening Center, including answers to frequently asked questions, please visit the Federal Bureau of Investigation's Web site at <http://www.fbi.gov/about-us/nsb/tsc>.

The U.S. Department of Homeland Security (DHS) has developed the Traveler Redress Inquiry Program (TRIP) to assist individuals who believe they have been incorrectly delayed, denied boarding, identified for additional screening, or have experienced difficulties when traveling. Although (b)(6) issues with Xerox Direct do not appear to be travel-related, applying for DHS TRIP may help to alleviate his concerns.

If (b)(6) would like to participate in the program, he should submit a Traveler Inquiry Form and requested copies of identity documents to DHS TRIP by applying online at [www.dhs.gov/trip](http://www.dhs.gov/trip) or by completing the enclosed form. DHS will review the information submitted and work with other Federal agencies, if necessary, to resolve individual concerns. DHS TRIP will inform (b)(6) in writing when review of his inquiry is complete.

We appreciate that (b)(6) took the time to share his concerns with you and hope this information is helpful. If we may be of further assistance, please call the Office of Legislative Affairs at (571) 227-2717.

Sincerely yours,

A handwritten signature in black ink that reads "Peter W. Hearing". The signature is written in a cursive, slightly slanted style.

Peter W. Hearing  
Deputy Assistant Administrator  
for Legislative Affairs

Enclosure



# Homeland Security

## Traveler Inquiry Form

### I. Your Travel Experience

Thank you for contacting the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP). Please check ALL scenarios that describe your travel experience:

- ☐ I am always subjected to additional screening when going through an airport security checkpoint
- ☐ I was denied boarding
- ☐ I am unable to print a boarding pass at the airport kiosk or at home
- ☐ I am directed to the ticket counter every time I fly
- ☐ The airline ticket agent stated that I am on a Federal Government Watch List
- ☐ I was detained during my travel experience
- ☐ A ticket agent took my identification and called someone before handing me a boarding pass
- ☐ I missed my flight while attempting to obtain a boarding pass
- ☐ I am repeatedly referred for secondary screening when clearing U.S. Customs and Border Protection
- ☐ I was denied entry into the United States
- ☐ I am a foreign student or exchange visitor who is unable to travel due to my status
- ☐ I was told my fingerprints were incorrect or of poor quality
- ☐ I feel I have been discriminated against by a government agent based on race, disability, religion, gender, or ethnicity
- ☐ I feel my personal information has been misused
- ☐ I was given an information sheet by a CBP Officer
- ☐ Other travel related issue

### II. Personal Information

Full Name:	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<i>First</i>	<i>Middle</i>	<i>Last</i>
Date of Birth:	<input type="text"/>	Place of Birth:	<input type="text"/>
	<i>mm/dd/yyyy</i>		<i>City or Town/Province/Country</i>
Sex:	<input type="checkbox"/> Male <input type="checkbox"/> Female	Height:	<input type="text"/>
		Weight:	<input type="text"/>
		Hair Color:	<input type="text"/>
		Eye Color:	<input type="text"/>

### III. Contact Information

Mailing Address:	<input type="text"/>		<input type="text"/>	
	<i>Street or PO Box</i>		<i>Apt. No.</i>	
Physical Address (if different):	<input type="text"/>		<input type="text"/>	<input type="text"/>
	<i>City or Town</i>		<i>State or Province</i>	<i>Zip or Postal Code</i>
	<input type="text"/>		<input type="text"/>	<input type="text"/>
	<i>Street</i>		<i>Apt. No.</i>	
Home Telephone:	<input type="text"/>		<input type="text"/>	
	<i>City or Town</i>		<i>State or Province</i>	<i>Zip or Postal Code</i>
E-mail Address:	<input type="text"/>		<input type="text"/>	
	<i>Work Telephone:</i>		<input type="text"/>	



# Homeland Security

## Traveler Inquiry Form

### IV. Additional Information (If applicable)

Date of Entry into U.S.: (mm/dd/yyyy)	/ /	Name of Airline or Ship:	
Port of Entry into U.S.:		Flight or Cruise Number:	
Departure Date from U.S.:	/ /	Other Names Used:	
U.S. Port of Departure:		Name at Entry into U.S.:	

### V. Required Documentation and Information

**U.S. citizens:** Please provide a legible, unexpired copy of a U.S. passport. If you do not have a U.S. passport, please provide at least one legible, unexpired copy of a government-issued identification document from the list below, preferably a photo ID. For minors (individuals under the age of 18), a copy of a certified birth certificate is the only identity document required.

**Non-U.S. citizens:** Please provide legible, unexpired copies of the biographical pages of your passport/travel document, and/or copies of any U.S. government-issued travel documents.

Check the box next to the document(s) you are submitting with this form:

Documentation	Information
<input type="checkbox"/> Passport	Registration No.: Country of Issuance:
<input type="checkbox"/> Passport Card	Number: Place of Issuance:
<input type="checkbox"/> Driver's License	License No. State of Issuance:
<input type="checkbox"/> Birth Certificate	Registration No. Place of Issuance:
<input type="checkbox"/> Military Identification Card	Number: Check one: <input type="checkbox"/> Air Force <input type="checkbox"/> Army <input type="checkbox"/> Marines <input type="checkbox"/> Navy <input type="checkbox"/> Coast Guard
<input type="checkbox"/> Government Identification Card	Number: Check one: <input type="checkbox"/> Federal <input type="checkbox"/> State <input type="checkbox"/> Local
<input type="checkbox"/> Certificate of Citizenship	Number: Place of Issuance:
<input type="checkbox"/> Naturalization Certificate	Number: State of Issuance Date: (mm/dd/yyyy) / /
<input type="checkbox"/> Immigrant/Non-Immigrant Visa	Number:
<input type="checkbox"/> Alien Registration	Number: Date: (mm/dd/yyyy) / /
<input type="checkbox"/> Petition or Claim Receipt	Number: Date: (mm/dd/yyyy) / /
<input type="checkbox"/> I-94 Admission	Number: Date: (mm/dd/yyyy) / /
<input type="checkbox"/> FAST	Number: Date: (mm/dd/yyyy) / /
<input type="checkbox"/> SENTRI	Number: Date: (mm/dd/yyyy) / /



# Homeland Security

## Traveler Inquiry Form

<input type="checkbox"/>	NEXUS	Number:	
		Date: (mm/dd/yyyy)	/ /
<input type="checkbox"/>	Border Crossing Card	Number:	
		Date: (mm/dd/yyyy)	/ /
<input type="checkbox"/>	SEVIS	Number:	
		Date: (mm/dd/yyyy)	/ /

### VI. Incident Details

Please briefly describe your travel experience:

------------------

### VII. Acknowledgement

The information I have provided on this application is true, complete, and correct to the best of my knowledge and is provided in good faith. I understand that knowingly and willfully making any materially false statement, or omission of a material fact, on this application can be punished by fine or imprisonment or both (see section 1001 of Title 18 United States Code).

I understand the above information and am voluntarily submitting this information to the Department of Homeland Security.

Date:	Full Name:	Signature:

**PAPERWORK REDUCTION ACT STATEMENT:** Through this information collection, DHS is gathering information about you to conduct redress procedures, as an individual who believes he or she has been (1) denied or delayed boarding, (2) denied or delayed entry into or departure from the United States as a port of entry, or (3) identified for additional screening at our Nation's transportation hubs, including airports, seaports, train stations and land borders. The public burden for this collection of information is estimated to be five minutes. This is a voluntary collection of information. If you have any comments on this form, you may contact the Transportation Security Administration, Office of Transportation Security Redress, TSA-901, 601 South 12<sup>th</sup> Street, Arlington, VA 20598-6901. An agency may not conduct or sponsor, and persons are not required to respond to, a collection of information unless it displays a currently valid OMB control number. The OMB control number assigned to this collection is 1652-0044.

**PRIVACY ACT NOTICE AUTHORITY:** Title IV of the Intelligence Reform and Terrorism Prevention Act of 2004 authorizes DHS to take security measures to protect travel, and under Subtitle B, Section 4012(1)(G), the Act directs DHS to provide appeal and correction opportunities for travelers whose information may be incorrect. Principal Purposes: DHS will use this information in order to assist you with seeking redress in connection with travel. Routine Uses: DHS will use and disclose this information to appropriate governmental agencies to verify your identity, distinguish your identity from that of another individual, such as someone included on a watch list, and/or address your redress request. Additionally, limited information may be shared with non-governmental entities, such as air carriers, where necessary for the sole purpose of carrying out your redress request. Disclosure: Furnishing this information is voluntary; however, the Department of Homeland Security may not be able to process your redress inquiry without the information requested.





**Homeland  
Security**

## **Traveler Inquiry Form**

**Please mail, fax, or e-mail your completed Traveler Inquiry Form and copies of identity documents to the Department of Homeland Security.**

**Mailing Instructions**

**Please mail the completed form and copies of identity documents to:**

**DHS Traveler Redress Inquiry Program (TRIP)**

**601 South 12th Street, TSA-901**

**Arlington, VA 20598-6901**

**E-mailing Instructions**

**Please e-mail the completed form and copies of identity documents to:**

**TRIP@dhs.gov**

FEB 20 2013

U.S. Department of Homeland Security  
601 South 12th Street  
Arlington, VA 20598

The Honorable Jeff Duncan  
U.S. House of Representatives  
Washington, DC 20515-4003



Transportation  
Security  
Administration

Dear Congressman Duncan:

Thank you for your letter of January 16, 2013, written on behalf of your constituent, (b)(6) regarding his concerns that his name may appear on a Federal watch list.

The Transportation Security Administration's (TSA) Secure Flight program conducts watch list matching for all passengers on flights from, to, and within the United States to identify individuals who may pose a threat to aviation or national security. As appropriate, Secure Flight identifies passengers for enhanced screening, law enforcement interview, or prohibition from boarding an aircraft.

Since its implementation, Secure Flight has demonstrated the value of uniform, consistent watch list matching through improved identification of matches to the watch list, thereby improving national security, preventing passenger misidentifications, and facilitating legitimate passenger air travel.

To further prevent passenger misidentifications, the U.S. Department of Homeland Security (DHS) has developed the Traveler Redress Inquiry Program (TRIP) to assist individuals who believe they have been incorrectly delayed, denied boarding, identified for additional screening, or have experienced difficulties when traveling.

TSA sent a letter to (b)(6) on February 20, 2013, explaining the availability of DHS TRIP. To participate in the program, travelers are asked to submit a completed Traveler Inquiry Form and requested copies of identity documents to DHS TRIP. DHS will review the information submitted and work with other Federal agencies, if necessary, to resolve individual concerns. DHS TRIP will inform (b)(6) in writing when review of his inquiry is complete.

We appreciate that (b)(6) took the time to share his concerns with you and hope this information is helpful. If we may be of further assistance, please call the Office of Legislative Affairs at (571) 227-2717.

Sincerely yours,

A handwritten signature in black ink that reads "Sarah Dietch".

Sarah Dietch  
Assistant Administrator  
for Legislative Affairs



**Homeland  
Security**

July 24, 2013

The Honorable Jeff Duncan  
Chairman  
Subcommittee on Oversight  
and Management Efficiency  
U.S. House of Representatives  
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your recent letter regarding the Federal Flight Deck Officer (FFDO) program.

The FFDO program was created by the *Arming Pilots Against Terrorism Act of 2003*, which authorizes the deputation of qualified airline pilots to act as federal law enforcement officers in order to defend the flight decks of aircraft against acts of criminal violence or air piracy. The Transportation Security Administration's (TSA) Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) is charged with oversight and management of this voluntary program.

The TSA Fiscal Year 2014 Budget contains no funding for the FFDO program. It is proposed the program will be funded by the airlines through a reimbursable agreement with the Federal Law Enforcement Training Center (FLETC) with training to be provided at FLETC sites.

TSA will continue to provide program oversight through monitoring and tracking firearms and firearm requalification, monitoring schedule changes of daily missions and resolving incidents. TSA will continue to find efficiencies within the FFDO program that will allow TSA to direct limited appropriated funding to risk-based programs.

I have enclosed a document addressing your inquiries. Thank you for your continued interest and support. Chairman Duncan will receive a separate, identical response. Should you need additional assistance, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Brian de Vallance".

Brian de Vallance  
Acting Assistant Secretary for Legislative Affairs

Enclosure



## Homeland Security

July 24, 2013

The Honorable Richard Hudson  
Chairman  
Subcommittee on Transportation Security  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your recent letter regarding the Federal Flight Deck Officer (FFDO) program.

The FFDO program was created by the *Arming Pilots Against Terrorism Act of 2003*, which authorizes the deputation of qualified airline pilots to act as federal law enforcement officers in order to defend the flight decks of aircraft against acts of criminal violence or air piracy. The Transportation Security Administration's (TSA) Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) is charged with oversight and management of this voluntary program.

The TSA Fiscal Year 2014 Budget contains no funding for the FFDO program. It is proposed the program will be funded by the airlines through a reimbursable agreement with the Federal Law Enforcement Training Center (FLETC) with training to be provided at FLETC sites.

TSA will continue to provide program oversight through monitoring and tracking firearms and firearm requalification, monitoring schedule changes of daily missions and resolving incidents. TSA will continue to find efficiencies within the FFDO program that will allow TSA to direct limited appropriated funding to risk-based programs.

I have enclosed a document addressing your inquiries. Thank you for your continued interest and support. Chairman Duncan will receive a separate, identical response. Should you need additional assistance, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Brian de Vallance", with a long horizontal line extending to the right.

Brian de Vallance  
Acting Assistant Secretary for Legislative Affairs

Enclosure



## Homeland Security

July 15, 2013

The Honorable Richard Hudson  
Chairman  
Subcommittee on Transportation Security  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your recent letter to Secretary Napolitano regarding explosives detection research and development data developed as part of the Transportation Security Administration's (TSA) canine breeding program.

TSA's Office of Law Enforcement/Federal Air Marshal Service is charged with procurement, training, and certification of TSA explosives detection canines while the Department of Homeland Security's (DHS) Science & Technology Directorate (S&T) works to identify opportunities for strategic partnership with existing programs and provides academic and scientific support across the Homeland Security Enterprise. Below are our responses to your inquiries.

- 1. How does your Department plan to continue utilizing the research and development gained under TSA's canine breeding program at Lackland Air Force Base?**

The research and development conducted by DHS S&T in partnership with TSA validated the success of TSA's selective breeding methods and identified certain key behavior indicators that will have direct benefit to the canine detection community.

- 2. Do you currently have plans to transfer the program to DHS S&T or partner with another entity, such as an academic institution? If so, what is the timeline for that transition?**

The Honorable Richard Hudson

Page 2

Since 2009, TSA has partnered with S&T to shape our requirements. The goal is to collectively identify opportunities for strategic partnerships with existing canine programs and academic institutions in order to better position DHS to leverage current research and development, including breeding efforts.

TSA is working with S&T to determine the best mechanism to transfer TSA canine breeding program research data to an interested private sector or academic partner and is in the process of conducting a feasibility and legal review. However, S&T will continue to maintain its research and development program and partnerships to maintain ongoing support to DHS canine teams.

Thank you for your continued interest and support. Representative Rogers, who co-signed your letter, will receive a separate, identical response. Should you need additional assistance, please do not hesitate to contact me at (202) 447-5890.

Respectfully,

A handwritten signature in black ink, appearing to read "Brian de Vallance", with a long horizontal flourish extending to the right.

Brian de Vallance  
Acting Assistant Secretary for Legislative Affairs