Privacy Impact Assessment
for the

Department of Homeland Security
General Contact Lists

June 15, 2007

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

Many Department of Homeland Security operations and projects collect a minimal amount of contact information in order to distribute information and perform various other administrative tasks. Department Headquarters has conducted this privacy impact assessment because contact lists contain personally identifiable information.

Overview

The Department's mission encompasses a wide variety of activities, including: emergency response, law enforcement and intelligence, critical infrastructure protection, immigration processing, and research and development of new technologies. In order to facilitate the accomplishment of these activities the Department is in constant contact with the public as well as partners in other federal, state, local, and international governmental organizations (hereinafter known as "partners"). Part of the Department's interaction with the public and its partners involves the maintenance of very limited contact information. For example, a member of the public may request mail or email updates regarding emergency response procedures, or partners working on cross-agency project may need to be able to contact their peers. These types of situations require the exchange of minimal contact information in order to facilitate the Department's operations and service to the public.

Accordingly, DHS collects limited contact information such as name, email address, and mailing address. Many times names and phone numbers are not required for mass distribution lists. Other times name and business affiliation, in addition to basic contact information, will be collected in order to facilitate a working relationship between partners.

General information intake involves the following:

An individual person will contact the Department via phone, paper form, or electronically (web or email) for the purpose of being added to an information distribution list. In order to accommodate that request, the person will provide basic contact information (depending on the circumstances) such as his or her name, mailing address, email address, and phone number. DHS then places the contact information in a spreadsheet, database or other type of information management tool. The Department then accesses the information from its storage site and uses it to distribute information or contact users per the confines of their interaction with DHS.

The authority to collect the information lies within each program or project's authorizing legislation.

Any program or project seeking to use this PIA as privacy documentation for its contact list must meet the following requirements:

1. The contact information is limited to non-sensitive personally identifiable information. An example of sensitive personally identifiable information is the social security number or date of birth.
2. The program or project must affirm that the document or database in which the contact information is stored resides on a system that has received an Authority to Operate from the Chief Information Security Officer.
3. The program or project must affirm that user access controls are in place governing who may view

or access the contact information. The contact information must not be universally accessible.

4. The contact information must only be used for the purpose for which it originally was collected, i.e., to contact individuals. Any additional sharing or use will require a separate PIA.

Should a program or project feel its contact list meets these requirements, the program or project is required to complete a Privacy Threshold Analysis (PTA) detailing how it has met these requirements. Once the PTA is approved, the program or project's name and component will be added to Appendix B of this document as a qualifying program or project.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

Contact lists generally include name, business affiliation, mailing address, phone number, and email address. Sensitive personally identifying information such as a social security number or date of birth are not covered under this PIA. Such collections are required to conduct separate PIAs analyzing the risks associated with such sensitive collections.

1.2 What are the sources of the information in the system?

Information is collected directly from individuals seeking information from the Department, or who are working collaboratively with the Department on various projects. Individuals provide their information voluntarily.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information is collected to facilitate the dissemination of information regarding the Department's operations and to facilitate the collaboration of partners who are working with the Department on various projects.

1.4 How is the information collected?

Information may be collected electronically, by paper form, or by telephone.

1.5 How will the information be checked for accuracy?

Information is collected directly from individuals who volunteer information and is assumed to be accurate. Depending on the context of the collection, the project or program may conduct a certain degree of verification of information and follow up with an individual if information is found to be inaccurate.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Programs are at a minimum authorized to collect and maintain contact information by the Homeland Security Act of 2002. Specific legal authorities for this type of collection are established based on each component and each program's particular mission. Nonetheless, some programs may operate under specific rules, regulations, treaties, or other statutes pertinent to their field.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The privacy risk presented by a basic contact list is that more information will be collected than is necessary to distribute information. Contact information is limited to the information necessary to perform the information distribution functions of the program or project. All information is collected with the consent of the individual.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The Department uses the information to contact individuals.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Information is stored but is not manipulated in any way other than to, if necessary, populate address fields for a mass email or paper mailing. Data may be input into databases or electronic spreadsheets and accessed via the various data elements. For example, a query may be conducted to locate all contacts in a certain state.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Contact lists are not created, populated with, or verified with data collected from commercial or publicly available sources.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The risk presented by the use of contact information is that the information would be used in ways outside the scope intended by the initial collection. Per the System of Records Notice DHS/All 002 (69 FR

70460, December 6, 2004) and the Privacy Act Statements given prior to collection, information collected for contact lists is not to be used for any other purpose than to contact individuals who have requested particular information. Additionally, all Department employees and contractors are trained on the appropriate use of personally identifiable information.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

The Department retains the information no longer than is useful for carrying out the information dissemination or collaboration purposes for which it was originally collected. Individuals may request their information be deleted if he or she is no longer interested in receiving information from the Department, after which point their information will not be retained. Absent a more restrictive retention period for a particular contact list, information is retained per the requirements of General Records Schedule 14, Informational Services Records (see Question 3.2).

3.2 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Records are retained and disposed of in accordance with the National Archives and Records Administration's General Records Schedule 14. Files may be retained for up to six years. For requests that result in litigation, the files related to that litigation will be retained for three years after final court adjudication.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Information is retained for no more than six years after the last use. This minimizes retention and security costs associated with maintaining contact lists. Additionally, any individual may opt out of any distribution list at any time in order to have their information expunged from the list, thereby eliminating any privacy risks posed by retention of their contact information.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Contact information may be shared with internal DHS components inasmuch as they are involved in distributing information or collaborating with partners within the Department. However, DHS does not share contact information for any purpose beyond which it was originally collected, i.e. contact information given by individuals for purpose *x* will not be shared for use of purpose *y* at a later date.

4.2 How is the information transmitted or disclosed?

DHS may share information by electronic or paper means. If information is transmitted electronically, proper security measures are taken, including encryption when necessary.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Inappropriate sharing is a risk inherent to any collection of personally identifiable information. Department employees and contractors are trained on the appropriate use and sharing of personally identifiable information. Further, any sharing of information must align with the purpose of the initial collection as well as the System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004) and the Privacy Act Statement provided at the time of collection.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Contact information may be shared with external governmental entities inasmuch as those entities are involved in distributing information or collaborating with partners within the Department. Nonetheless, contact information is not shared for any purpose beyond which it was originally collected, i.e. contact information given by individuals for purpose *x* will not be shared for use of purpose *y* at a later date.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes. Per the System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004) and the various notices provided when information is collected, uses of contact information beyond the purposes for which it was originally collected is not acceptable.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Any information shared with organizations outside the Department is required to be appropriately secured per Office of Management and Budget Memorandums 06-15, Safeguarding Personally Identifiable Information, and 06-16, Protection of Sensitive Agency Information.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

A risk is presented whenever the Department shares information it has initially collected from agencies or individuals outside of the Department. If external sharing of information would exceed the narrow purpose for which the contact information was collected, then the information is not permitted to be shared. The System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004) outlines the specific instances where contact information may be shared outside the Department. All Department employees and contractors are trained on the appropriate use and sharing of information.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Yes. This privacy impact assessment and the System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004) provide notice regarding the collection of contact information by the Department. More appropriately, though, each collection of contact information is immediately preceded by notice regarding the scope and purpose of the contact information at the time of collection. These Privacy Act Statements (these notices are required under 5 U.S.C. § 552a(e)(3)) at the moment of

collection provide individuals with notice of the voluntary nature of the collection and the authority to collect the information.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes. Individuals are not required to provide contact information. Nevertheless, if contact information is not provided individuals may not receive information from the Department or from partners in the Department.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

DHS will use the information only for the purposes for which it was collected, i.e., contacting individuals. Should an individual suspect information is being used beyond the given scope of the collection, they are encouraged to write to the system managers listed in Appendix A. The system managers are also listed in the System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004).

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The privacy risk associated with notice in the collection of contact information is that the individual is not aware of the purpose for which the information he or she submits may be used. This risk is primarily mitigated by limiting the use of contact information to what is necessary for the purposes of contacting the person according to his or her voluntary subscription or request. Additionally, the System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004) provides notice of the purpose of the collection, redress procedures and the routine uses associated with the collection of contact information. Notice is always provided prior to the collection of information, and consent is obtained by the individual prior to his providing information.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Should individuals seek to remove their name from a contact list they should write or call the program or project which initially collected the information. The program or project is in the best position to remove, edit and/or provide access to the information held on an individual. Access requests can also be directed to FOIA / PA D-3, The Privacy Office U.S. Department of Homeland Security, 245 Murray Drive SW, Building 410, STOP-0550, Washington, DC 20528-0550.

Additionally, the System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004) details

access provisions along with the names of officials designated to field such requests within the Department.

7.2 What are the procedures for correcting inaccurate or erroneous information?

The procedures are the same as those outlined in Question 7.1.The program or project that initially collected the information is in the best position to correct any inaccurate information. Any inquires for correction should be made to the initial collector.

Additionally, the System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004) details access provisions along with the names of officials designated to field such requests within the Department.

7.3 How are individuals notified of the procedures for correcting their information?

Individuals are notified at collection that they may correct their information at any time by the procedures outlined above.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Appropriate redress is provided.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Individuals may correct their information at any time during which the Department possesses and use their contact information. Any risks associated with correction of information are thoroughly mitigated by the individual's ability to opt out of the contact list or correct their information via the same process by which they submitted information.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

Departmental physical and information security policies dictate who may access Department computers and filing systems. Specifically, DHS Management Directive 4300A outlines information technology procedures for granting access to Department computers, which is where the majority of contact information is stored. Access to contact information is strictly limited by access controls to those who require it for completion of their official duties.

8.2 Will Department contractors have access to the system?

Yes, depending on the project or program. Many times contractors are tasked with information distribution and other outreach tasks. Contractors are required to have the same level of security clearance in order to access Department computers as all other DHS employees.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All Department employees and contractors are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of personally identifiable information such as what is contained in contact lists.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Most simple contact lists are stored on spreadsheets or similar formats that do not qualify as an information technology system requiring a Certification and Accreditation (C&A) pursuant to the review processes established by the Chief Information Security Officer; however, these documents are stored on secure Department networks which have completed C&As. Other contact lists which are part of more robust functionalities reside on information technology systems that are required to receive a C&A.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

All Department information systems are audited regularly to ensure appropriate use and access to information. Specifically related to contact information, such lists residing on a local area network's shared drive are restricted by access controls to those who require it for completion of their official duties. Folders within shared drives are privilege-protected.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The risk of unauthorized access exists with any information technology system or document. The Department conducts thorough background checks on every employee and contractor. Access to the systems and networks which store the contact information are protected pursuant to established Departmental procedures (see 8.4).

All Department employees and contractors are trained on security procedures, specifically as they relate to personally identifiable information.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

This assessment covers contact lists developed by a program or project involved in outreach efforts or collaboration efforts within or outside of the Department.

9.2 What stage of development is the system in and what project development lifecycle was used?

The program or projects detailed here are not necessarily involved in a specific lifecycle. Complete information technology systems are in the operational phase and have completed C&A documentation. Individual contact information lists do not have a development cycle.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

If a particular technology used in the collection or handling of information in connection with the types of contact lists addressed in this PIA raises specific and/or heightened privacy concerns, the implementation of the technology will be required to conduct a separate PIA.

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Appendix A

I. For Headquarters components of the Department of Homeland Security, the System Manager is the Director of Departmental Disclosure, U.S. Department of Homeland Security, Washington, DC 20528.

II. For operational components that comprise the U.S. Department of Homeland Security, the System Managers are as follows:

United States Coast Guard, FOIA Officer/PA System Manager, Commandant, CG-611, U.S. Coast Guard, 2100 2nd Street, SW., Washington, DC 20593-0001

United States Secret Service, FOIA Officer/PA System Manager Suite 3000, 950 H Street, NW., Washington, DC 20223

United States Citizenship and Immigration Services, ATTN: Records Services Branch (FOIA/PA), 111 Massachusetts Avenue, NW, 2nd Floor, Washington, DC 20529

National Protection and Programs Directorate, FOIA Office, 3801 Nebraska Ave., NW, Nebraska Avenue Complex, Washington DC 20528

United States Customs and Border Protection, FOIA Officer/PA System Manager, Disclosure Law Branch, Office of Regulations & Rulings, Ronald Reagan Building, 1300 Pennsylvania Avenue, NW (Mint Annex)., Washington, DC 20229

United States Immigration and Customs Enforcement, FOIA Officer/PA System Manager, Office of Investigation, Chester Arthur Building (CAB), 425 I Street, NW., Room 4038, Washington, DC 20538

Transportation Security Administration, FOIA Officer/PA System Manager, Office of Security, West Building, 4th Floor, Room 432-N, TSA-20, 601 South 12th Street, Arlington, VA 22202-4220

Federal Protective Service, FOIA Officer/PA System Manager, 1800 F Street, NW., Suite 2341, Washington, DC 20405

Federal Law Enforcement Training Center, Disclosure Officer, 1131 Chapel Crossing Road, Building 94, Glynco, GA 31524

Under Secretary for Science & Technology, FOIA Officer/PA System Manager, Washington, DC 20528

Office of Intelligence and Analysis, 3801 Nebraska Ave., NW, Nebraska Avenue Complex, Washington DC 20528

Under Secretary for Management, FOIA Officer/PA System Manager, 7th and D Streets, SW., Room 4082, Washington, DC 20472

Office of Inspector General, Records Management Officer, Washington, DC 20528

Appendix B

Qualifying Programs or Projects

DHS Advance Acquisition Plan/Acquisition Forecast System

The Advance Acquisition Plan/Acquisition Forecast system will facilitate the collection, review, approval and management of Advance Acquisition Plans in accordance with the FAR, HSAR, and HSAM. In addition, it will provide the acquisition forecast that supports the Office of the Small and Disadvantaged Business Utilization in its efforts to help publish business opportunities available to small businesses.

DHS Headquarters Avaya PBX Systems (DAPS)

The purpose of the DHS Avaya PBX Systems (DAPS) is to provide DHS end users with telephone and voicemail services. The PBX bestows incoming and outgoing call processing for various DHS locations.

DHS Sunflower Asset Management System (SAMS)

SAMS is an asset management system used for tracking the personal property of the Department of Homeland Security (DHS).

DHS NOC S&L Support Desk

The NOC S&L Support Desk monitors state and local homeland security incidents and works closely with the NOC, I&A and IGA to coordinate issues of significance to their constituencies. It receives, tracks, and responds to requests (by telephone and email) directed to DHS from those elected or appointed officials in accordance with the existing I&A Single Point of Service (SPS) process.

DHS Recovery Act Data Warehouse

The DHS Recovery Act Data Warehouse will be a repository used to fulfill a number of reporting requirements on all DHS associated Recover Act Grants awarded.

Federal Emergency Management Agency Application for Surplus Federal Real Property

The Support Services and Facilities Management Division (SSFMD) uses FEMA Form 60-25 (currently titled, (*Excess Real Property Application for Public Benefit Conveyances*) in the collection of data to process applications for Public Benefit Conveyance (PBC) and Base Realignment And Closure (BRAC) programs whereby approved State and Local government applicants may acquire Federal property to use for emergency management purposes.

Federal Emergency Management Agency Debris Removal Contractor Registry

The Debris Contractor Registry (DCR) is a tool for local governmental entities to more easily identify and contact debris removal contractor resources for pre-planning or post-disaster response purposes. The objectives of the DCR system are to allow debris contactors to register online and to allow the public to search through the registry of debris contractors.

Federal Emergency Management Agency IMSG Port Security Grant Program

The overall purpose of the PSG is to provide a single point-of-entry for the Office of Grants & Training (G&T) grantees (state and local jurisdictions) and grantors (G&T staff) of grant expenditures. The PSG is a web-based solution providing grantees the ability to report on their grant funding allocations and, where applicable, their performance metrics.

Federal Emergency Management Agency National Fire Academy Long-Term Evaluation

The National Fire Academy regularly surveys students and their supervisors on the long term impacts of NFA training on Fire and EMS departments and organizations.This voluntary survey (O.M.B. No. 1660-0039 - Expires March 31, 2009), formerly paper-based, will now be conducted through the U.S. Fire Administration Web site.

Federal Emergency Management Agency National Fire Department Census

The National Fire Department Census project seeks to identify fire departments in the U.S. and their various characteristics regarding demographics, capabilities, and activities.The database will be used to guide programmatic decisions and provide information to the public.

Federal Emergency Management Agency USFA Web Farm

The USFA Web Farm is a website application using Microsoft, Cold Fusion Oracle solution that is integrated into the public web server architecture http://www.usfa.fema.gov.The application directly supports the dissemination and availability of information for the general public to protect lives and property from fire related hazards.

Federal Emergency Management Agency Private Sector Division Professional Contact Information Lists

The PSDPCIL system conducts outreach to the private sector and works with internal DHS and FEMA partners to coordinate private sector outreach efforts.The system retaines internal and external professional contact information.

I&A Contact Database Tool

The Contact Database Tool (CDT) is an "electronic Rolodex™" of contact information for persons and organizations who have requested intelligence products from DHS.The contact information is used to deliver finished intelligence products to the proper recipient in the form and format requested by the customer.Contact information is also used to identify and locate persons who should review and provide editorial comments to draft intelligence products. The review and comment process is commonly referred to as "vetting".

I&A Customer Feedback Program

DHS I&A collects feedback from its customers through an electronic questionnaire attached to each of its products. The OMB-approved questionnaire, DHS Form 6001, is designed to elicit voluntary feedback on the impact and relevance of, as well as ways to improve, the intelligence product for our customers.

I&A Customer Feedback Program

The IS&C (Information Sharing and Collaboration) Stakeholder Database assists branch staff in increasing the consistency of interaction with key stakeholders of the Information Sharing Environment, to include DHS staff, other federal, state, and local entities, and private sector individuals.

ICE Academy Class Management System

The Academy Class Management System (ACMS) is a legacy INS web-based application that supports and processes law enforcement student training data for ICE, Federal Protective Services (FPS) and Customs and Border Protection (CBP).

ICE IMAGE Information Request & Membership Application Form

The ICE Mutual Agreement between Government and Employers (IMAGE) program is the outreach and education component of the Office of Investigations (OI) worksite enforcement (WSE) program. Under this program, ICE will partner with businesses representing a broad cross-section of industries. Businesses must adhere to a series of best practices, enroll in E-Verify, and complete an IMAGE Membership Application form.

ICE Task Management System (TMS)

The ICE OCIO Chief of Staff (CoS) needs a task management system (TMS) to manage the receipt, creation, distribution, tracking, archival, and disposition of tasks/assignments across the OCIO organization. The tasks come from a diverse source which includes internal divisions of ICE, DHS Headquarters and other components of DHS, external agencies, Congress and the White House.

Infrastructure DHS Interactive

The purpose of the Department of Homeland Security Interactive Portal (DHSI) is to provide a public facing Internet portal that is used to disseminate and coordinate information with other external organizations that work closely with DHS in planning and conducting Homeland Security activities. The system also provides access to private areas that can be used in all phases of an emergency or disaster including access to references, plans, and collaboration tools.

Infrastructure GovDelivery content subscription service

This service allows citizens to opt‐in for notifications which they can subscribe for off of public internet sites. It is an automated system that uses e‐mail to notify citizens on the specific topics they have subscribed. Information that the GovDelivery service hosts would be the e‐mail address & subscription preferences.

National Protection and Programs Directorate 2010 Chemical Sector Security Summit

DHS and the Chemical Sector Coordinating Council are co‐sponsoring the 2010 Chemical Sector Security Summit. This Summit is designed for industry professionals throughout the entire chemical sector involved with corporate and facility security; environment, health and safety; and the transportation and distribution of chemical products.

National Protection and Programs Directorate Infrastructure Information Collection Program

The Infrastructure Information Collection Program (IICP) supports the requirements for collecting, cataloguing, and maintaining standardized and quantifiable infrastructure information to enable the execution of national risk management for CI/KR and for prioritizing the data for use by homeland security partners.

National Protection and Programs Directorate Master Station Log

The primary purpose of the Master Station Log is to provide the Watch Analysts of the National Coordinating Center (NCC) with the capability to gather and retain historic reference of communication (phone, email, and verbal) between National Coordinating Center Communications Information Sharing Analysis Center (COMM-ISAC) members. The MSL provides continuing records of the Watch's daily operation as well as serve as a tracking device for the demands and requests placed on the Watch.

National Protection and Programs Directorate Meridian Conference Website 2009

Registration website for the Meridian conference - a conference focused on International awareness and collaboration in regard to the Critical Information Infrastructure Protection (CIIP) for countries around the world. The purpose of this site will be to present general information in regard to the conference and the conference topics, as well as to provide a registration page for those interested in attending.

National Protection and Programs Directorate Mission Operating Environment

The Secure Mission Operating Environment (SOME) comprises 4 stand alone workstations that will become a dedicated closed TS/SCI operational system. This system will perform analysis and support a relational database that will track trends across all of the DHS components.

National Protection and Programs Directorate RAMCAP System

As required by Homeland Security Presidential Directive – 7 (HSPD-7), DHS developed the National Infrastructure Protection Plan (NIPP) to facilitate the identification, prioritization, and coordination of the protection of the nation's Critical Infrastructure and Key Resources (CI/KR). RAMCAP is both a process and system that informs the National Strategic Risk Assessment which identifies and prioritizes critical assets across the seventeen (17) CI/KR sectors.

National Protection and Programs Directorate Share Resources High Frequency Program

The purpose of SHARES is to provide a single, interagency emergency message handling system by bringing together existing HF radio resources of Federal, state and industry organizations when normal communications are destroyed or unavailable for the transmission of national security and emergency preparedness information. The SHARES program is a coordination of activities, not an IT system.

National Protection and Programs Directorate Telecommunications Service Priority (TSP) Web

The TSP Web enables the TSP PO to manage TSP user access, generate notices and reports, schedule and execute batch procedures for TSP Web data processing, create and execute SQL queries, maintain Telecommunications Service Priority Authorization Codes, Federal Information Processing Standards (FIPS) Codes, maintain point of contact and organization information, perform TSP database administrative tasks, and fulfill Federal Communications Commission (FCC) reporting requirements.

National Protection and Programs Directorate Vehicle-Borne Explosive Device (VBIED) Training

DHS Office of Infrastructure Protection, as the Chemical Sector - Specific Agency, in collaboration with the Protective Security Coordination Divisions Office of Bombing Prevention will provide the Vehicle Borne Improvised Explosive Device (VBIED) Training Program for Chemical Facilities.

National Protection and Programs Directorate Vulnerability Identification Self Assessment

The Vulnerability Identification Self Assessment Tool (ViSAT) is a program that develops methodologies and standards for non - complex infrastructure through the use of scalable common metrics which enables cross - sector risk comparisons. ViSAT performs calculations based on metrics.

National Protection and Programs Directorate Next Generation network (NGN) Priority Service Program

Next Generation Network Priority Service Program (NGN PTS) collects information to verify the existence and approval of a priority user access request or the identity of an authorized user so that

support (in the form of information about NGN PTS) can be provided, and collaboration (between NGN PTS and priority users impacted by the transition) can be enhanced.

National Protection and Programs Directorate Chemical Security Awareness Training Program

The purpose of the Chemical Security Awareness Training Program (CSATP) is to increase the level of security awareness among general employees of chemical facilities and to enhance the security of the United States.

National Protection and Programs Directorate General Meetings Registration and Post-Meeting Survey (GMRE)

The General Meeting Registration and Post-Meeting Survey (GMRE) is designed to support the planning of meetings, workshops, and other outreach events and activities hosted by the office in fulfillment of its statutory mandate to conduct extensive nationwide outreach outlined in the Homeland Security Act of 2002, 6 U.S.C. § 101 et seq.

National Protection and Programs Directorate Technical Assistance Request and Evaluation (TARE)

In order for the Office of Emergency Communications to assess the value of the services it provides through technical assistance, an evaluation form is also requested of those receiving technical assistance.

National Protection and Programs Directorate National Cybersecurity Awareness Campaign, PSA Challenge

The National Cybersecurity Awareness Campaign is putting out a call to all citizens to prepare a video public service announcement for the National Campaign to potentially use on its website and its federal partners website. Individuals will have to provide information so they may be notified that their entry has been chosen.

NETC Learning Resource Center (NETCLRC)

The mission of the Learning Resource Center is to support the instructional activities of the National Emergency Training Center (NETC) with exemplary library and information services. Since the LRC is organizationally positioned in the US Fire Administration National Fire Data Center, the LRC emphasizes its services to the National Fire Academy students and our Nations fire service personnel.

Office of Health Affairs (OHA) Email Distribution Lists

The project will allow recipients of e‐mails through the OHA Distribution List to limit the emails they receive from OHA to only DHS‐related matters, only OHA‐related matters, or to completely opt out of receiving any future correspondence from OHA. This is intended to ensure that OHA sends information to only those individuals who wish to receive it.

Operations Directorate Personnel/COOP Database

It is a stand alone database used to prepare and maintain a roster of personnel needed to ensure a minimum level of performance of the organization's essential functions.

Private Sector Engagement:Human Trafficking

PSO toolkit is used to discuss the issue of human trafficking and introduces private sector partners to the Blue Campaign, DHS's coordinated effort to combat trafficking in persons. Companies are invited to submit an email request for more information on human trafficking or report suspected instances

Science and Technology Attendance Lists

S&T staff regularly hold meetings, conferences, working groups, and workshops on topics related to homeland security. In order to plan conferences, S&T employees and contractors create and maintain attendance lists.

Science and Technology Biodefense Knowledge Center (BKC) Subject Matter Expert (SME) Directory

The DHS Biodefense Knowledge Center (BKC) is developing a biological agent Subject Matter Expert (SME) Directory to provide government and approved contractor personnel a rapid means of identifying biological agent SMEs. This database is necessary to identify SMEs who can voluntarily assist with peer review of individual assessments and scientific programs, including meetings held in support of Department of Homeland Security (DHS) Biological Threat Risk Assessments and Population Threat Assessments, and who can provide scientific expertise during a perceived biothreat event.

Science and Technology BioWatch Web-Portal

The BioWatch Portal (BW Portal) is an access restricted, secure Web portal that gives users the ability to access program information and resources, share BioWatch information, work in collaborative environments, and experience lessons learned with peers from around the country.

Science and Technology Cyber Security Research and Development Center Web Site

The Cyber Security R&D Center (CSRDC) is a government industry partnership to protect the information security of the U.S. critical infrastructure, the vast majority of which is in the private sector. The Center is the primary vehicle through which the DHS Science and Technology Directorate plans and executes its cyber security R&D programs.

Science and Technology Media Contact List

S&T maintains a media contact list for the purposes of distributing press materials. S&T also maintains publication mailing lists for the purposes of distributing (via e‐mail and postal mail) program materials.

Science and Technology Multi-Band Radio Project

DHS S&T ▪ s Office for Interoperability and Compatibility (OIC) Multi‐Band Radio Project will further develop and test a prototype multi‐band, multi‐mode portable radio capable of providing uninterrupted communications between local, tribal, state, and Federal emergency response agencies operating in the various public safety radio bands.

Science and Technology National Bio and Agro-Defense Facility (NBAF) Web page

Because the decision whether to build and site the NBAF is a major Federal action, the Science and Technology Directorate is managing the preparation of an environmental impact statement (EIS) under the National Environmental Policy Act (NEPA). NEPA requires engaging potential stakeholders and inviting comment during the scoping period and upon publication of the draft EIS.

Science and Technology Private Sector Contact Lists

The CCO maintains lists of business contact information for private sector firms that have expressed an interest in participating in S&T - funded projects. The CCO also receives unsolicited proposals and ideas, which also contain contact information.

Science and Technology Project Execution System

PES is a project management system tool that enhances project management, portfolio balance, and reporting of research and development funds. HFD will perform a usability study using volunteers from the End User community (program managers internal to DHS S&T).

Science and Technology Subject-Matter Expert Lists

S&T staff create and maintain lists of subject - matter experts throughout government, academia, and the private sector. The individuals on these lists are experts in areas related to homeland security research and development and are regularly consulted to provide input for S&T projects and initiatives.

Science and Technology Technical Evaluation System for Safety Act

TESSA is a legacy system that has recently been replaced by the SAFETY Act Management System (SAMS). TESSA is being retained for historical data validation purposes. The SAFETY Act allows companies and individuals from the private sector to apply for insurance liability protection for anti-terrorism products and services.

Science and Technology This Week in Science and Technology (TWIST)

This Week in Science and Technology (TWIST) registration provides DHS personnel (employees and contractors) with access to a weekly one hour live webcast and chat room discussing scientific initiatives and programs from S&T.

Science and Technology Treaty Compliance Database

Database compiling DHS - sponsored biological and chemical defense programs. The purpose of the database is to store comprehensive information on each program (types of select agents, toxins, chemicals used; technical approach; description of research, etc.).

Science and Techonology Centron

The Centron software/hardware system provides critical monitoring of incubators, refrigerators, freezers, and animal rooms to ensure the devices are within the standard operating temperatures set by the PIADC research staff. The Centron software will be used to keep track of temperature values in key instruments used in validating vaccine trials.

Transportation Security Administration Contact Center

The TSA Contact Center's Transportation Inquiry Processing Management System (TCC V.2) is comprised of various information technology systems, mechanisms, and databases designed to manage all agency inquiries from the general public and TSA employees and contractors. They form an inter-connected configuration of information technology, IT and communication tools that are owned by TSA but managed by an off-site contractors.

Transportation Security Administration Enterprise Performance Management Platform (EPMP) PMIS/PIMS

This is primarily an internal TSA system used to track and analyze operational data. PMIS is an Internet-based tool designed to primarily collect, report, and perform analyses on transportation security

status and progress, beginning with data on security, equipment, and screening activities from TSA's aviation security activities.

Transportation Security Administration Grants Blog

This blog is sponsored by the Transportation Security Administration to facilitate an ongoing dialogue on innovations in security, technology and the checkpoint screening process.

Transportation Security Administration Highway & Motor Carriers Corporate Security Review System

The Highway and Motor Carrier Division of the TSA Transportation Sector Network Management Division (TSNM - HMC) is developing the HMC - CSR System for the Corporate Security Review (CSR) Management System. The CSR is an instructive review that provides the TSA TSNM - HMC with a general understanding of motor carrier, motor coach, and school bus owner/operators ability to protect its critical assets.

Transportation Security Administration Inquiry Management System (IMS)

IMS is a web-based application that tracks and manages call inquiries received by the CRC that includes inquirer contact information and inquiry details.

Transportation Security Administration Intermodal Security Training and Exercise Program (I-STEP) Exercise Information System (EXIS)

The Exercise Information System (EXIS) is an Internet - accessible knowledge management system serving all stakeholders – industry, port authorities, federal agencies, and state and local governments – and integrating all Intermodal Security Training Exercise Program (I - STEP) components at the sensitive security information level. It gives stakeholders valuable exercise information tailored to the transportation industry, and gives developers best practices and past work for use in future exercises.

Transportation Security Administration Performance Information Management System (PIMS)

PIMS allows TSA to meet its missions through the generation of timely, thorough performance measures, metrics, and operational reports. This is primarily an internal TSA system used to track and analyze operational data, but it also occasionally houses public contact information on those who are seeking recovery of lost and found items.

Transportation Security Administration Pipeline Security Guidelines

As part of the Pipeline Security Guidelines, TSA recommends that each pipeline operator establish and implement a risk-based plan to address and document the organization's policies and procedures for managing security related threats, incidents, and responses.

Transportation Security Administration Rail Security

The Final Rule (rule), published November 10, 2008, establishes security requirements for freight railroad carriers; intercity, commuter, and short - haul passenger train service providers; rail transit systems; and rail operations at certain, fixed - site facilities that ship or receive specified hazardous materials by rail.

Transportation Security Administration Security Training Programs for Surface Mode Employees

The Transportation Security Administration (TSA) proposes employee security training program requirements for surface modes of transportation. These include freight railroad carriers, public transportation agencies (including rail mass transit and bus systems), passenger railroad carriers, over‐the‐road bus operators, and motor carriers transporting Highway Security‐Sensitive Materials (HSSM).

Transportation Security Administration Travel Protocol Office Program

The Transportation Security Administration (TSA) has established the Travel Protocol Office (TPO) to support and facilitate the movement of eligible travelers through the airport security screening process. Eligible travelers are persons whose presence at a screening checkpoint may pose undue risk or distraction to other travelers and the screening process.

Transportation Security Administration Liaisons Divisions Database

Database containing the names, phone numbers, mailing address and email addresses of law enforcement, air carrier, and international transportation security stakeholders that the Liaison Division interacts with or may interact with concerning TSA/Office of Law Enforcement matters.

Transportation Security Administration Ad Hoc Reporting

The Ad Hoc Reporting tool is a data-driven technology available to TSA applications residing on the HTMLDB that allows TSA application administrators/users to tailor reports of the data contained in their specific application.

Transportation Security Administration Contact Center

The TSA Contact Center's Transportation Inquiry Processing Management System (TCC v3) is comprised of various information technology systems, mechanisms, and databases designed to manage all agency inquiries from the general public and TSA employees and contractors.

U.S. Coast Guard 2009 World Maritime Day Parallel Event

The purpose of this request for PTA is to set up a registration website at www.uscg.mil. The audience for the event will include national and international dignitaries including government and industry members.

U.S. Coast Guard List Server (CGLS)

CGLS is a mailing list manager, which allows elements within the USCG to send notices via electronic mail (e-mail) out to a one-way mailing list, available for subscription to the public.

U.S. Coast Guard Navigation Systems Information Dissemination Network (NSIDN)

The purpose of the General support System (GSS) Navigation Systems Information Dissemination Network (NSIDN) is to disseminate navigation safety information to the public via the Internet.

U.S. Coast Guard Proceedings magazine online subscription request form

In support of the U.S. Coast Guard Marine Safety and Security Council and as a service to its potential subscribers, Proceedings of the Marine Safety and Security Council, the Coast Guard Journal of Safety and Security at Sea, seeks to add an online subscription request form to its website.

United States Citizenship and Immigration Services Customer Service Portal Alert by Mail

The purpose of CSWP is to simplify customer access to USCIS information and services through a consolidated and integrated service website. This web service provides web users with the ability subscribe to a particular piece of website content and receive an email when that content is updated.

United States Citizenship and Immigration Services Customer Service Portal Forms by Mail

The Customer Service Web Portal (CSWP) Forms by Mail allows web users to request for USCIS immigration form(s) through the official USCIS website. The web user voluntarily provides his/her full name, company/title, and mailing address to receive the requested immigration form(s) in the mail. USCIS uses the collected information to mail the immigration forms.

United States Citizenship and Immigration Services Enterprise Portal

The Enterprise Portal system will serve as the conduit for customers to interact with USCIS. The USCIS Enterprise Portal will, upon completion, and over several phases, encompass all existing Web sites providing information under the purview of USCIS, and will continually expand to include any new E‐Government information or services provided by USCIS (e.g., e‐filing and other paperwork reduction act (PRA) initiatives).

United States Citizenship and Immigration Services Edify System

The USCIS Northeast Regional Office uses the Edify application to manage incoming calls requesting forms from USCIS. The Edify application records incoming calls and an operator transcribes the message and saves the full name, address, and forms requested to a database for fulfillment and tracking purposes. This enables the operator to print the name and address on an envelope to send USCIS forms to the requestor.

United States Citizenship and Immigration Services Teachers of English to Speakers of Other Languages (TESOL) Conference Booth Follow Up List

We will have a booth at the 43rd annual Teachers of English to Speakers of Other Languages (TESOL) Conference in Denver, CO in March, 2009, where we will have sample copies on hand and will give away a limited number of our publications at the event. To maximize resources, we want to avoid shipping excessive copies of our educational publications to the conference location. Instead, we would like to collect participant contact information during the conference so we can ship copies of our materials upon return to Washington, DC.

United States Coast Guard Citizen's Action Network

The Citizen's Action Network was designed to create a database of volunteers who live near navigable waterways that can be called upon to help the Coast Guard investigate cases such as flare sightings or mayday calls in their area.

United States Secret Service CPNI Reporting

The CPNIReporting Web site is co‐sponsored and managed by the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI). The web site is a tool for telecommunications carriers to report a breach of its customer's CPNI (customer proprietary network information) to law enforcement.

DHS National Information Exchange Model (NIEM)

The purpose of the NIEM project is to provide a customer relationship management platform that enables the program management office the ability to perform and integrate contact management, stakeholder management, event registration, helpdesk issue tracking and project tracking functions.