Privacy Impact Assessment
for the

Department of Homeland Security
General Contact Lists

DHS/ALL/PIA-006

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

For more information on additional programs that fall under this PIA, see below or reach out to the appropriate Component Privacy Office with any questions.

- **U.S. Customs and Border Protection (CBP):** Privacy.CBP@cbp.dhs.gov
- **Cybersecurity and Infrastructure Security Agency (CISA):** Privacy@cisa.dhs.gov
- **Department-wide Programs (DHS) or other Components or offices not listed:** Privacy@HQ.DHS.GOV
- **Federal Emergency Management Agency (FEMA):** FEMA-Privacy@fema.dhs.gov
- **U.S. Immigration and Customs Enforcement (ICE):** ICEPrivacy@dhs.gov
- **Office of Intelligence and Analysis (I&A):** IAIntelOversight@HQ.DHS.GOV
- **Science and Technology (S&T) Directorate:** stprivacy@HQ.DHS.GOV
- **U.S. Citizenship and Immigration Services (USCIS):** USCIS.PrivacyCompliance@uscis.dhs.gov
- **U.S. Coast Guard (USCG):** HQS-DG-M-CG-61-PII@uscg.mil
- **U.S. Secret Service (USSS):** privacyservicesprogram@USSS.DHS.GOV
- **Transportation Security Administration (TSA):** TSAPrivacy@tsa.dhs.gov

Qualifying Programs or Projects (ordered by component by date)

Customs and Border Protection (CBP):

CBP Program Management and Reporting System (PMRS)

PMRS is a prototype lifecycle management system used by the Office of Finance to track real estate, facilities, maintenance, and project & portfolio management for personal and real property. Please note that the DHS/ALL-010 DHS Asset Management Records SORN, 80 FR 58280 (September 28, 2015) covers this collection. (January 5, 2011)

CBP Situation Management System (SMS)

The Situation Management System (SMS) shares incident information in real time through message boards that transmit data about emergencies amongst CBP authorized personnel, as well as between CBP and Federal, state, local, tribal, and international agencies through the Joint Operations Directorate Incident Command Center. (June 28, 2013)

Cybersecurity and Infrastructure Security Agency (CISA) (formerly National Protection and Programs Directorate (NPPD))

The Cybersecurity and Infrastructure Security Agency Act of 2018 was signed by President Trump on 11/16/18, renaming NPPD to CISA. All previous NPPD entries are now under CISA.

1670-NEW SAFECOM Membership Questionnaire

The purpose of the SAFECOM Expertise and Experience Questionnaire is to obtain actionable and critical data that drives emergency communication policies, programs, and funding. SAFECOM works with federal and emergency response stakeholders to improve providers' communications and interoperability. (July 7, 2020)

2020 Vulnerability Management Technical Exchange (2020 VM TE)

The purpose of the 2020 Vulnerability Management Technical Exchange (2020 VM TE) is to promote the VM mission and collaboration against cyberattacks. The 2020 VM TE will (1) advance knowledge sharing with the public and private VM community, (2) discuss future VM capabilities and (3) improve awareness of CISA services. (June 29, 2020)

DHS/CISA Annual National Cybersecurity Summit

The Annual National Cybersecurity Summit is voluntary; there is no charge to register or attend; and the event where government, academia, and industry partners gather to protect critical infrastructure. Registration is through Eventbrite and CISA collects information at the time of registration to thank attendees, answer questions, and/or inquire about future CISA events. Eventbrite will collect the registrant's information, only CISA will use the disclosed information, and will deleted the registrant's information from the database at the conclusion of the event.

NRMC Elections Security Initiative and Countering Foreign Influence Product Focus Groups

The purpose of the National Risk Management Center (NRMC) Elections Security Initiative (ESI) and Countering Foreign Influence (CFI) Product Focus Groups is to enhance public awareness of risks to the nation's critical function, one of which is the elections. The NRMC is an organization within CISA, ESI and CFI are within NRMC, and the focus group involves a CISA information collection (July 13, 2020)

The President's Cup Cybersecurity Competition

The purpose of The President's Cup Cybersecurity Competition is aimed to identify, recognize, and reward the best cybersecurity talent in the federal executive workforce. The President's Cup is open to all individual Federal Executive Branch cybersecurity practitioners, including the Department of Defense (DoD) and Uniformed Services as well as teams of up to five members within each department, agency, or uniformed service. Government contractors are not eligible to participate in the President's Cup. (June 25, 2020)

Tardis

Tardis is an incident management system that streamlines internal and external communication. The data within Tardis can only accessed by CISA\Threat Hunting, customers do not access, and customers can only provide information that goes into it. Tardis does not distribute information and information about one customer is not directly provided to another. (July 28, 2020)

US-CERT Forms.US-CERT.gov Website

The purpose of the Forms.US-CERT.GOV website is to support US-CERTs mission by serving as a communication channel to disseminate technical details of Internet threats. This vehicle allows both the government, public, and private sector to report suspicious activity. (January 2, 2010)

NPPD Chemical Sector Security Summit

DHS and the Chemical Sector Coordinating Council are co-sponsoring the annual 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. (April 26, 2019)

NPPD 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. (April 19, 2010)

NPPD 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. (May 27, 2010)

NPPD 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. (October 20, 2010)

NPPD Priority Telecommunications Service (PTS) Program

The Priority Telecommunications Service Program leverages commercially owned networks to provide specially designed telecommunications services to National Security and Emergency Preparedness users during natural or man-made disasters when conventional communications services are ineffective. General contact information is collected for users and then used to provide service notification and programmatic information to the POCs. (December 9, 2010)

NPPD 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. (June 14, 2011)

NPPD 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. (March 29, 2012)

NPPD Sector Outreach Activities Contact Lists.

The Office of Infrastructure Protection, Sector Outreach and Programs Division (SOPD) oversees the Department's support of partnership councils, education and outreach, planning and preparedness exercises, and information sharing related to critical infrastructure protection and resilience. SOPD will collect and maintain contact information from other Federal, state, local, tribal and territorial entities, and public and private owners and operators of critical infrastructures to distribute sector-related information and newsletters to stakeholders, as well as to register participants for exercises, webinars, trainings, and meetings, including Critical Infrastructure Partnership Advisory Council meetings and events. (October 21, 2013).

Interagency Security Committee Compliance System (ISC-CS).

The ISC-CS offers Federal departments and agencies a centralized, secure database that provides an analytical capability, allowing authorized ISC-CS users to query the database based on selected criteria and produce reports that provide insight into compliance of participating Federal facilities. The ISC-CS system provides a dashboard capability to visualize the results of analytics about key risk features and status of Federal Facilities against these features. ISC-CS creates contact lists from the collection of name, email address, phone number, Department/Agency, and Bureau provided by the requestor to verify the accuracy of information on form submissions and helpdesk inquiries. ISC-CS uses the Office of Management and Budget's (OMB) MAX Authentication Services, and the attributes passed back from OMB MAX during authentication will not be stored in a method that allows the information to be retrieved by personal identifiers. (November 29, 2018)

Department-wide Programs (DHS):

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). (March 13, 2012)

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. (November 4, 2009)

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. (April 28, 2010)

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. (July 27, 2010)

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. (November 2, 2010)

DHS Service Catalog

The DHS Service Catalog will provide a 'One Button' shopping experience from selecting, ordering, fulfillment, and provisioning of products and services. The Enterprise Service Catalog will focus on identifying products and services associated with Enterprise Licenses, IT Services & Hardware catalog developed by the Office of the Chief Information Officer (OCIO), and provide the Office of the Chief Procurement Officer (OCPO), Strategic Sourcing with an automated solution that allows users throughout DHS to search and acquire commodities in the DHS environment. (February 17, 2011)

Domestic Nuclear Detection Office (DNDO):

DNDO Bids/Small Business Innovative Research (DNDOBids/SBIR)

DNDOBids/SBIR is a proposal management support system that provides a facility through which vendors may submit whitepapers and proposals to DNDO for evaluation. DNDO collects contact information from vendors including names, addresses, telephone numbers, e-mail addresses, and organizational affiliation for the purposes of contacting vendors and their representatives regarding their submissions through DNDOBids/SBIR. Please note that the DHS/ALL-021 Department of Homeland Security Contractors and Consultants SORN, October 23, 2008, 73 FR 63179 covers this collection. (January 18, 2011)

Federal Emergency Management Agency (FEMA):

FEMA Hub of Philanthropic Engagement Service Provider Questionnaire

The FEMA Hub of Philanthropic Engagement is a public/private partnership initiated to help meet needs caused by 2017 hurricanes in Puerto Rico. The Hub works across Puerto Rico to connect philanthropies and community-based service providers to bridge gaps in recovery funding, technical resources, and material goods. The purpose of the questionnaire is to collect information about service provider organizations and build a database of non-profit organizations across all sectors working on recovery in Puerto Rico. (November, 2018)

FEMA 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. (April 17, 2007)

FEMA 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), formerly paper-based, will now be conducted through the U.S. Fire Administration Web site. (June 19, 2008)

FEMA 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. (June 20, 2008)

FEMA 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. (September 17, 2009)

FEMA 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. (October 7, 2009)

FEMA 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. (November 17, 2009)

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. (April 5, 2010)

FEMA 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. (August 20, 2010)

FEMA Logistics Information Management System (LIMS)

LIMS is FEMA's single property management system. The system manages maintenance and material supporting Mobile Emergency Response Support (MERS) teams. Additionally, LIMS tracks all FEMA property, property custodians, and physical location of stored proerty. Please note that the DHS/ALL-010 Department of Homeland Security Asset Management Records SORN, 80 FR 58280 (September 28, 2015) covers this collection. (January 27, 2011)

FEMA Chemical Stockpile Emergency Preparedness Program (CSEPP) Evaluation and Customer Satisfaction Survey

The Chemical Stockpile Emergency Preparedness Program (CSEPP) is one facet of the multi-hazard readiness program dealing with the potential of chemical spills or releases into the communities surrounding the seven U.S. chemical stockpiles (known as CSEPP sites). The program's goal is to improve preparedness to protect the people of these communities in the unlikely event of an accident involving this country's stockpiles of obsolete chemical munitions. FEMA collects the evaluation data through telephone surveys. The questions are aimed at assessing public knowledge of emergency preparedness and response actions in the event of a chemical emergency affecting any of the seven CSEPP sites. (July 6, 2011)

FEMA Federal Assistance for Offsite Radiological Emergency Planning

Pursuant to 44 CFR 352.5 FEMA is required to respond to any Nuclear Regulatory Commission (NRC) licensee that may request use of FEMA-owned/managed resources during a Radiological Emergency Preparedness (REP) exercise. The licensee must submit their request for resources in written statement to the host FEMA Regional Office. (November 23, 2011)

FEMA Form 516-0-1 Federal Hotel and Motel Fire Safety Declaration Form

FEMA United States Fire Administration uses FEMA Form 516-0-1, The Federal Hotel and Motel Fire Safety Declaration Form, to collect basic information on life-safety systems related directly to fire-safety in hotels, motels, and similar places of accommodation applying for inclusion on the National Master List (NML). The form requests specific responses from applicants as to the installation of smoke detectors in all guestrooms of properties submitted for listing on the NML. (January 24, 2012)

FEMA Building Code Adoption Tracking Losses Avoided Studies/Hazus

The Building Science Branch of FEMA's Mitigation Branch is performing a study of the effect of building code adoption and enforcement on the losses avoided in some select communities around the nation in order to compare, contrast, and evaluate the effectiveness of communities' efforts. These pilot studies can help to develop a general methodological approach to quantifying the losse4s avoided through building code adoption and enforcement. (March 28, 2012)

FEMA Industry Liaison Program (ILP) - Vendor Information Collection

FEMA's ILP – Vendor Information Collection is the point of entry for vendors seeking to do business with FEMA. During disasters, vendor request to work with FEMA may quadruple, negatively impacting FEMAs capacity tom immediately respond to such inquiries related to the provision of disaster-related services. To address this issue, FEMA has created its FEMA Form 516-0-0-3, "Industry Liaison Program Vendor

Profile," to facilitate appropriate meeting opportunities with FEMA wherein the vendors present their capabilities to FEMA programs. (March 29, 2012)

FEMA Total Records Information Management (TRIM)

TRIM is an electronic records management system operated by the Mitigation Directorate within the Federal Insurance and Mitigation Administration (FIMA). TRIM stores records/documents limited to specific FIMA program areas and do not include all FIMA records. There are existing Systems of Records Notices and Routine Uses, which cover the records maintained with the TRIM system. (May 3, 2012)

FEMA National Business Emergency Operations Center (NBEOC)

The NBEOC Contacts List maintains the basic contact information of FEMA's private sector/business community stakeholders. The NBEOC Contacts List will facilitate DHS to community communication as well as facilitate consent to share with others to enhance disaster response and recovery operations. (May 18, 2012)

FEMA National Flood Insurance Program (NFIP)-Community Information System (CIS)

The CIS, as the database system is commonly called, provides information about floodplain management, mapping and insurance for the NFIP participating communities. The CIS includes demographic, engineering, insurance and community specific information for jurisdictions in the United States that are identified as flood prone. CIS is an integrated application that is comprised of discrete modules and standard reports. (May 24, 2012)

FEMA All Hazards Position Specific Instructor Website

The National Incident Management System (NIMS) Incident Command System (ICS) All-Hazards Position Specific training program located at FEMA Emergency Management Institute (EMI)/National Emergency Training Center (NETC) currently maintains a website as required to support the program. In addition to introductory program information, the site contains links to class schedules, course materials, a training video, and a listing of qualified instructors (name and contact information) used by federal, state, and local officials for the selection of instructors for various courses. (June 8, 2012)

FEMA GovDelivery Content Subscription Service

The GovDelivery service allows the public to opt-in for email notifications from FEMA. It is an automated system that uses e-mail to notify the public on the specific topics they have opted to receive emails about. Upon registration users are taken to an external site hosted by the GovDelivery company that manages the subscription list. Individuals are then asked to provide their email address, select how they would like to receive emails (immediately, daily digests, or weekly digests), an optional password for managing their subscriptions, their selection of issues and topics they are interested in learning about, and an optional zip code. (June 8, 2012)

FEMA READY.gov and LISTO.gov

The primary objective of the Ready.gov and its Spanish language version Listo.gov is to provide the public with information concerning current disasters and emergency preparedness. The Ready.gov website is comprised of read-only, static content that is updated on a regular basis. Ready.gov is a national public

service advertising (PSA) campaign designed to educate and empower Americans to prepare for and respond to emergencies including natural and man-made disasters. The goal of Ready.gov is to foster public involvement and ultimately increase the level of basic preparedness across the nation. Individuals have the option to submit their email addresses to receive a monthly newsletter or email updates. (May 17, 2013)

Immigration and Customs Enforcement (ICE):

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. (January 8, 2010)

Office of the Chief Information Officer (OCIO) Business Process System (O-BPS)

O-BPS is a SharePoint application that automates OCIO's task management process. O-BPS manages the receipt, creation, distribution, tracking, archival, and disposition of tasks across OCIO. O-BPS also manages the OCIO Workforce Management Division (WMD) hiring process, including tracking staffing needs, managing position announcements, and managing the direct hire and incentives process. O-BPS collects and maintains general, business contact information about individuals submitting tasks/requests and ICE employees and contractors assigned tasks. The information is only used within ICE OCIO. (September 21, 2016)

Office of Intelligence and Analysis (I&A):

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. (May 19, 2010)

I&A Information Sharing and Collaboration Stakeholder Database

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. (October 5, 2010)

I&A Communications Security (COMSEC) Program

I&A's COMSEC Program manages COMSEC material and equipment issued to DHS employees, contractors, state/local/tribal law enforcement and private sector. I&A collects minimal contact information to identify who and where the asset is assigned (name, office location and phone number). Please note that

the DHS/ALL-010 - DHS Asset Management Records SORN, 80 FR 58280 (September 28, 2015) covers this collection. (December 28, 2010)

I&A Foreign Disclosure Log

I&A maintains a record of all requests for release of DHS intelligence information to and by foreign partners. In support of this requirement I&A has established an Access Database entitled Foreign Disclosure Log (Log). The Log contains contact information (name, work phone number, work e-mail address) of the DHS staff member requesting the information release and the contact information and country of the recipient. (February 8, 2011)

I&A Interagency Remote Sensing Coordination Cell

The Interagency Remote Sensing Coordination Cell Executive Secretariat maintains a contact list to fulfill an advisory function and coordinate with various U.S. Government points of contact to support remote sensing-related homeland security missions. (February 8, 2011)

I&A Intelligence Training Branch Mission Liaison Data Files

I&A maintains official points of contact within State and Local Fusion Centers responsible for coordinating the nomination and follow-through with eligible State and Local Fusion Center staff candidates for I&A-provided training activities. (February 25, 2011)

I&A Intelligence Training Branch Student Data Files

I&A provides, as appropriate, training to authorized individuals external to DHS. Students include federal, state, local, and foreign national officials. Students provide contact information to allow for the coordination of training activities. (February 25, 2011)

Management (MGMT):

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. (July 21, 2009)

Office of the Chief Security Officer (OCSO):

Succession Planning Tool

It is a stand-alone database used to maintain a roster of all OCSO personnel. (May 28, 2014)

Office of Health Affairs (OHA):

OHA Email Distribution Lists

The project will allow recipients of emails 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. (January 7, 2010)

BioWatch Database

BioWatch is an early detection system designed to provide, maintain, and support a continuous bio-aerosol threat monitoring capability in selected metropolitan areas. The BioWatch database contains contact information of individuals on the federal and local level working on the BioWatch program. (June 3, 2011)

Chemical Defense Demonstration Projects

DHS OHA, Health Threats Resilience Division (HTR), Chemical Defense Program (CDP) will initiate, fund, and manage two chemical defense demonstration projects in selected state, local, territorial, or tribal (SLTT) venues. The Congressional Report for the FY 2012 Appropriations Act providing funds for the demonstration projects requires that OHA competitively select the demonstration project sites. As the demonstration projects will not be funded through contract or grant/cooperative agreement mechanisms, there is not an established method of determining interested and appropriate SLTT venues. Therefore, OHA will issue a Notice Requesting Expressions of Interest in the *Federal Register* that will allow SLTT agencies and venues to express and detail their interest in participating in the demonstration projects. In providing a submission in response to the Notice, SLTT agencies and venues will need to provide contact information as well as an explanation of their interest and details as to why the specific venue meets the requirements for the demonstration project. (June 28, 2012)

Office of Operations Coordination and Planning (OPS):

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. (July 26, 2010)

DHS Red Phone Database

The DHS Red Phone Database enables the DHS Private Sector Office (PSO) to collaborate with private sector entities by obtaining updated contact information for the timely sharing of in-depth, concise, and

tailored information during an emergency incident. The provision of contact information is voluntary and private sector partners my opt-out at any time. (June 29, 2011)

OPS Detailee Affairs Program (DAP) Database

The OPS Detailee Affairs Program (DAP) Database is used to continuously monitor the status of inbound, outbound, and on-site detailees for OPS. The contact information contained in the OPS DAP Database will ensure effective in-processing and out-processing of such detailees and is the sole repository for information for the Quarterly Congressional Detailee Report. (September 29, 2011)

OPS Support Request (SR) Database

The SR Database is a central repository that allows the OPS SR project team to collect, compile, and store DHS support requests and track their status from Department of Defense (DOD) Joint Task Force North (JTF-N) and the National Guard Bureau (NGB). The database collects the name and office phone number from DHS POCs at CBP, ICE, and USCG, and from DOD/NGB POCs. The PIA allows for collection of information for distribution purposes, and to perform various other administrative tasks. PII is collected from DHS employees as well as anyone considered to be a DHS "partner," which includes other federal organizations such as DOD and NGB. (March 19, 2013)

Office of Policy (PLCY)

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. (October 31, 2007)

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. (June 4, 2010)

Science & Technology (S&T):

S&T 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. (January 19, 2010)

S&T 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. (July 9, 2010)

S&T 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.). (November 23, 2010)

S&T Defense Technology Experimental Research (DETER)

The S&T Cyber Security Division sponsors the DETER testbed for conducting research and experimentation of malicious Internet software (malware). The testbed facilitates scientific experimentation and validation against established baselines of attack behavior and supports innovative approaches that involve breaking the network infrastructure. (April 7, 2011)

S&T 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. (April 29, 2011)

S&T 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. (June 14, 2011)

DHS Supported Student Data Collection Initiative

The DHS S&T Office of University Programs (OUP) currently administers several programs and initiatives that assist in increasing the Homeland Security (HS) Science, Technology, Engineering, and Math (STEM) workforce. Collectively, these programs and initiatives are intended to inspire, engage, educate and ultimately direct academically high performing individuals toward choosing HS-STEM related careers. In attempt to better evaluate the success of our programs we would like to pursue a project to collect information on students supported through grants and individual awards from DHS S&T Office University Programs (OUP). (March 22, 2012)

Small Business Innovation Research (SBIR) and Broad Agency Announcement (BAA)

The DHS S&T SBIR-BAA is a web based that publishes DHS Science and Technology (S&T) Small Business Innovation Research (SBIR) and Broad Agency Announcement (BAA) solicitations. The system allows companies to download solicitation documentation, as well as submit proposals online in response to those solicitations. S&T uses the system to conduct reviews and evaluate proposals. (October 20, 2009)

S&T Laboratory Network (LabNet)

The LabNet General Support System (GSS) provides a Research & Development focused network that allows greater freedom for researchers and scientists by limiting restrictions with regard to systems and software. While LabNet is more open than DHS-managed networks, there are also controls, policies and procedures in place to provide an adequate level of information assurance. The LabNet GSS contains redundant Active Directory servers that store limited PII, including: username, password, location, email address, job role, and phone number. LabNet also collects audit and log information for the LabNet Wireless Guest VLAN Collaboration Workspace and LabNet GSS. This information is monitored by the LabNet Security Operations Center (SOC) and includes username (first name.last name). This information is also used to generate reports. For annual training requirements a user's first name, last names, and title (government / contractor) are extracted from Active Directory to identify all active users on the LabNet GSS.

S&T Project 25 Compliance Assessment Program (P25 CAP)

The P25 CAP is a formal, independent process for ensuring communications equipment declared by the supplier actually is interoperable with other compliant devices, regardless of manufacturer. Specifically, this voluntary program provides public safety agencies with evidence that the communications equipment they purchase is tested against and complies with the P25 standards for performance, conformance, and interoperability. Compliance testing concludes with official Summary Test Reports and Suppliers' Declaration of Compliance documents. These documents are submitted to DHS via email. P25 requests full name, work email, work phone number, and a signature for the manufacturer point of contact. Once the SDOC is posted, the manufacturer point of contact's name, work email, work phone number, and signature are available through the website. (October 23, 2018)

S&T Incident Management Information Sharing (IMIS) Capability Maturity Model (CMM)

The IMIS CMM is an assessment framework for determining a First Responder organization's level of information sharing capability (Assessment). Assessments are conducted via an online web-application in the assessment taker's web browser. Assessments are performed at the entity level, not the personnel level. The data from the aggregated assessments will be used to help the Government understand national trends in information sharing capabilities and help aid federal grant making agencies in developing their programs and priorities. IMIS CMM collects the email addresses of the assessors. (October 31, 2018)

S&T Transportation Security Lab (TSL) Summer Intern and Visiting Scientist Program (SI/VSP)

DHS S&T established the Transportation Security Lab (TSL) Summer Intern and Visiting Scientist Program (SI/VSP) to enable students (summer interns), postdoctoral scientists and engineers, and visiting professors (visiting scientists) to work temporarily at the TSL on funded research and development programs. The TSL works with the U.S. Department of Energy (DOE) Oak Ridge Institute for Science and Education (ORISE), a DOE institute managed and operated by Oak Ridge Associated Universities (ORAU), a 501(c)(3) not for profit organization. S&T and DOE entered into a specific interagency agreement for ORISE assistance in staffing the TSL SI/VSP. (July 9, 2020)

FIND Mobile Application and FIND Software

DHS S&T funded dbS Productions to develop the FIND Mobile Application, a commercial mobile application that allows first responders involved with ground search and rescue operations to visualize

where a lost person is likely located. The mobile application, designed to operate on a mobile smartphone, tablet, or Android device, will be made available to the public via retail mobile software distribution platforms. Prior to the mobile application's commercialization, DHS S&T and dbS Productions will sponsor a series of mock search and rescue exercises for volunteer first responders to evaluate the mobile application and requires the collection of business contact information for logistical purposes. Although the app was developed with funding from DHS S&T, no information collected, used, or stored by the mobile application will be shared with DHS S&T for any purpose. (July 31, 2020)

Transportation Security Administration (TSA):

TSA 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). (November 24, 2009)

TSA 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. (December 2, 2009)

TSA 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. (January 8, 2010)

TSA 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. (May 27, 2010)

TSA 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. (August 10, 2010)

TSA Liaisons Divisions Database

This is a 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. (September 7, 2010)

TSA 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. (September 8, 2010)

TSA Security Manager/Coordinator Contact Lists

Security Manager/Coordinator Contact Lists collect contact information for security managers or coordinators at facilities across the United States, and in some instances, foreign countries. The provision of contact information is sometimes requested by regulation, but the information may also be provided informally for day-to-day ease of use between TSA and its stakeholders. (December 20, 2010)

TSA BlackBerry Executive Contact List (ECL)

This generates a contact list to which executives have access on their blackberries. (May 18, 2011)

TSA Can I Bring (CIB)

Can I Bring (CIB) contains a list of items that passengers can carry on, check in, or cannot bring to the airport. (May 18, 2011)

TSA Certified Cargo Screening Facilities Tracker (CCSFT)

This program prepares and certifies Certified Cargo Screening Facilities (CCSFs), which are industry facilities responsible for securing all cargo traveling on passenger aircraft. (May 18, 2011)

TSA Commercial Airlines FAQ (COMAIR_FAQ)

This provides a central database to manage DHS/TSA employee frequently asked questions and their answers for the Transportation Security Network Management (TSNM) Commercial Airlines division (May 18, 2011)

TSA Commercial Airlines PSI Reporting Database (PSI)

The "PSI" tool will serve as TSA's Commercial Airports tracker to record Principal Security Inspector (TSA employees & contractors) and aircraft operator security-related activities. (May 18, 2011)

TSA Configuration Management Automation System (CMAS)

CMAS was designed for the Office of Human Capital as a central system to organize change requests and to support configuration management of their HR software applications. (May 18, 2011)

TSA Daily Awareness Report (DAR)

This provides a single location to provide project status updates to Office of Information Technology (OIT) leadership. (May 18, 2011)

TSA DNS Registry (DNS_Registry)

This stores requests for new web addresses which, if approved, could become entries in the TSANET DNS servers. (May 18, 2011)

TSA Enhanced Staffing Model (ESM)

This is a web-based application that will allow TSA its users to perform the following functions: Model the number of TSA staffers needed to accomplish the screening workload at checkpoints and bag zones for a given airport configuration, compute the optimal number of staff (full time, part-time) needed to meet a given demand forecast for each airport terminal, and generate reports that display the various statistics generated during the modeling process (such as average and maximum delays, wait times, performance times). (May 18, 2011)

TSA Everything Database on .NET (EDB.NET)

This is an application developed to create simple web-based database applications quickly. (May 18, 2011)

TSA Freight Rail Contacts (FRC)

This manages a list of Security Coordinator contacts in the Freight Rail industry. (May 18, 2011)

TSA General Aviation 12-5 Profile Maintenance (TFSSP)

This manages profile information for GA Aviation Operator Security Coordinators (AOSC) for general aviation aircraft over 12,500 pound (12-5). (May 18, 2011)

TSA HQ Parking (HQ Parking)

HQ Parking processes individual headquarter parking payments for TSA employees and contractors. The process can relate to an individual as it handles parker information, information about their cars, as well as payment information. (May 18, 2011)

TSA IdeaFactory (IdeaFactory)

IdeaFactory (IdeaFactory) is an application that is part of the MOP_Apps system. Ideafactory is TSA's web site for employee collaboration on TSA's most important issues. (May 18, 2011)

TSA JobSwap (JobSwap)

JobSwap is a web-based application that allows Transportation Security Officers (TSOs) to collaboratively organize a voluntary job transfer. (May 18, 2011)

TSA Law Enforcement Officers Flying Armed (LEOFA)

The LEOFA application was developed to process and record armed Law Enforcement Officers (LEO) requests for access to a sterile area of an airport in order to board a flight. (May 18, 2011)

TSA OASIS Time Tracker (OASIS_Time)

OASIS TimeTracker provides a system for contractors to enter their hours worked against a defined set of projects and applications. (May 18, 2011)

TSA Peer Review (PEERREV)

The Peer Review Program (PRP), under the Office of Human Capital (OHC) of TSA, provides covered employees - Transportation Security Officers (including master and expert TSOs), Leads, and Supervisors with an alternative option to TSA's existing grievance and appeal processes. (May 18, 2011)

TSA Revenue Division Airline Contact Log (Revenue)

The Revenue application supports the Revenue division to track interactions with their stakeholders. (May 18, 2011)

TSA Screening Procedures Branch FAQ (SPB_FAQ)

Screening Procedures Branch FAQ (SPB_FAQ) provides a central database to manage TSA employee frequently asked questions and their answers for the OSO Screening Procedures division. (May 18, 2011)

TSA SIG Asset Management (SIGAM)

This application allows Office of Information Technology (OIT) to manage assignment of government information technology resources to individual employees and contractors. (May 18, 2011)

TSA SPOT Base Rate Study (SPOT_BRS)

Pilot program that is part of the Screening of Passengers by Observation Techniques (SPOT) Program designed to test the feasibility of adding new observation criteria to the SPOT_TDC application. (May 18, 2011)

TSA Unsolicited Proposal (ACQUP)

This application tracks Unsolicited Proposals submitted by individuals, companies, or organizations wishing to conduct business with TSA. (May 18, 2011)

TSA National Deployment Office (NDO) - Deployment Management System (DMS)

Deployment operations are planned and executed through the use of the NDO-DMS in support of numerous domestic airports and other venues based on seasonal demands, special events, local hiring shortfalls, or other circumstances requiring more staffing resources than are locally available. (May 18, 2011)

TSA OSO National Transfer (OSONVT)

OSONVT will provide a web-based application that includes new reporting, tracking and accountability requirements of the TSO National Voluntary Transfer Pilot Program. (May 18, 2011)

TSA FAMS Amber Alert Dissemination System (AmberAlerts)

This program is a voluntary partnership between law-enforcement agencies, broadcasters, and transportation agencies to activate an urgent bulletin in the most serious child-abduction cases. (May 18, 2011)

TSA Claims Management System (CMS) Status (CMS_Status)

Claims Management System is a public-facing website that allows claimants to search for the status of a pending claim. (May 18, 2011)

TSA Contact Us (ContactUs)

Contact Us is a web site that allows end users to fill out a form and submit it to a specific office via email. Forms are maintained by an admin group, and they can be created, deleted and changed dynamically by members of this group. (May 18, 2011)

TSA MyTSA Mobile Web Service (MyTSA_Mobile)

This application is designed to keep users with mobile devices such as an iPhone, or Blackberry up-to-date about airport delays, security checkpoint wait times. (May 18, 2011)

TSA Pay.Gov OCI Handler (Pay.Gov)

Pay.Gov is designed to facilitate a common method to make secure electronic payments to US Federal Government Agencies. This application is the TSA method to use the Pay.Gov system. (May 18, 2011)

TSA TalkToTSA (TalkToTSA)

Talk To TSA (formerly “Got Feedback” is a public-facing web application (App) that collects feedback from the traveling public and emails it to the Office of Strategic Communications and Public Affairs. (May 18, 2011)

TSA Vovici (Vovici)

Vovici Survey Workbench is a commercial product that allows licensed TSA personnel to create and execute surveys. (May 18, 2011)

TSA Liaison Division Databases -Law Enforcement Section - Air Carrier Section - International Section

This is a 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. (May 18, 2011)

TSA Sensitive Security Information Branch Phoenix Database

The TSA SSI Branch Phoenix Database serves as the repository for all information associated with document reviews undertaken by the SSI Branch. (May 18, 2011)

TSA Security Manager/Coordinator Contact Lists

TSA's security mission covers several modes of the transportation sector. In each mode, TSA regularly collects contact information for security managers or coordinators at facilities across the United States and in some instances foreign countries. (May 18, 2011)

TSA Highway Baseline Assessments for Security Enhancements (HWY BASE) System

The HWY BASE System provides TSA's Highway and Motor Carrier (HMC) Branch with an understanding of surface transportation stakeholders' (e.g., school bus owners/operators) ability to protect its critical assets. As part of conducting a transportation security review, TSA interviews individuals associated with private and commercial entities, who voluntarily provide limited business contact information so that TSA may collaborate and share with those points of contact the review results. TSA may also share management reports, including the contact information, with other federal agencies that participate in this process (e.g., Department of Transportation). (October 18, 2012)

TSA Pipeline Security Guidelines

As part of the risk-based plan in the Pipeline Security Guidelines, TSA recommends that natural gas and hazardous liquid pipeline owners and operators voluntarily provide TSA with 24/7 contact information of the primary and alternate security manager, and the telephone number of the company's security operations or control center. TSA uses this information, including the name, telephone number, and email address, to contact such personnel in the event of a change in security threat indicators and/or security incidents involving the pipeline. (October 18, 2012)

TSA Contact Center

The TSA Contact Center (TCC) v3 manages all agency inquiries from the public and TSA employees and contractors. The TCC allows individuals to provide comments to TSA through a web form or call into the TCC. A valid email address is required; however, any other information provided, including names, is voluntary. (December 10, 2012)

TSA TV Studio

Employees and contractors of TSA, DHS, and other federal agencies use TV Studio to produce and broadcast various multimedia events. TSA collects names and work phone numbers and email addresses, as well as consent forms from individuals who participate in these events. (May 29, 2014)

United States Coast Guard (USCG):

USCG 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. (March 27, 2009)

USCG 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. (August 17, 2010)

USCG 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 by the public. CGLS collects and maintains email addresses for those subscribed to the email lists available. The lists currently available include such subjects as policy and regulation changes for various USCG elements, USCG NavCen information for the public (i.e. daily GPS info). Information originates from list owners as an email that is sent to the appropriate list, which is then disseminated to the subscribed email addresses. (September 6, 2011)

USCG Integrated Aids to Navigation Information System (I-ATONIS)

There are five components of I-ATONIS used to collect personal information: Private Aid to Navigation Owner Contact Information, Wreck Owner Contact Information, Oil Rig Owner Contact Information, Private Property Owner Contact Information, and U.S. Coast Guard Auxiliary Member Contact Information. I-ATONIS stores information which allows the Coast Guard to contact owners of wrecks, oil rigs, private aids to navigation, private property owners on which an aid to navigation is located, and operators of oil rigs. If the owner designates another individual as the point of contact for the Coast Guard with respect to the wreck, oil rig, private aid, or leased property, the point of contact information is retained as well. (February 17, 2012)

USCG 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. (March 6, 2012)

USCG 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. (March 6, 2012)

Navigation Systems Information Dissemination Network (NSIDN)

The NSIDN disseminates navigation safety information to the public via the Internet. Website users may also register to receive products and notifications via email. (September 17, 2012)

U.S. Citizenship and Immigration Services (USCIS):

USCIS 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). (October 19, 2006)

USCIS Customer Service Portal

The Customer Service Web Portal (CSWP) serves as USCIS's primary information vehicle on the Internet. 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 customers the ability to find changes in USCIS policies and procedures, learn how to submit an application or petition, and obtain information about field offices. CSWP now consolidates information collected from USCIS.gov, E-Verify.gov, the Forms by Mail application, the FOIA Web Status Check, and the Congressional Website. (November 23, 2018)

USCIS 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. (September 2, 2010)

USCIS Japan Tsunami Incident Management Group (IMG)

The USCIS Japan Tsunami IMG is an email distribution list that was created in response to the Japan Tsunami disaster as an efficient and effective tool to coordinate responses by USCIS to official DHS requests for information related to the disaster. (June 15, 2011)

USCIS Form N-660, Application for Recognition as an American Institution of Research and Form N-660A, Notification of Material Changes

Form N-660 and N-660A allow organizations to apply for and maintain recognition as an American institution of research (AIR). These forms collect limited contact information from organization representatives to assist in the AIR recognition approval process. (December 20, 2012)

USCIS BIA Recognition & Accreditation Tracker

USCIS provides recommendations to the Department of Justice on Board of Immigration Appeals recognized organization and accredited representative applications. USCIS maintains limited contact information on organization representatives to assist in the recommendation process. (January 31, 2014)

USCIS Civics and Citizenship Toolkit Registration Form

USCIS provides one free Civics and Citizenship Toolkit to organizations that assist immigrants. The Toolkit contains a variety of educational materials designed to help permanent residents learn more about the United States and prepare for the naturalization process. This online registration form (at

www.uscis.gov/citizenshiptoolkit) is used to collect information on the organization's eligibility and their shipping address. (August 2, 2016)

USCIS Form G-1190, Free Training for Civics and Citizenship Teachers of Adults

The USCIS Office of Citizenship conducts teacher training events for adult citizenship instructors to enhance the skills needed to prepare immigrants for U.S. citizenship. To register for a training opportunity in an area, individuals complete and submit G-1190 to USCIS. USCIS uses the information to register the individual for the training. The information may also be used to share additional citizenship-related products, resources, and training opportunities from USCIS. USCIS provides individuals with the opportunity to opt out of receiving this additional information. (September 26, 2017)

USCIS Form G-1482, Citizenship and Integration Grant Program, Notice of Funding Opportunity

USCIS Citizenship and Integration Grant Program provides citizenship preparation resources, support, and information to immigrants and immigrant-serving organizations. Recipients of the Grant are public or private nonprofit organizations with recent experience providing citizenship instruction and naturalization application services to eligible permanent residents. Applicants to the Citizenship and Integration Grant Program are required to submit responses to G-1482. (September 21, 2016)

USCIS Field Operations Directorate Link (FODLink)

FODLink is a mobile application that provides an executive dashboard for use on mobile devices. FODLink accesses USCIS SharePoint sites to provide data access in real time. One of FODLink's functionalities is the Emergency Contact Module. FODLink provides emergency contact information for field officers and senior management, which includes employee contact information and work schedule. In case of a disaster or unfortunate event, managers have the emergency contact list available to them if they need to contact their employees. (January 3, 2018)

USCIS Form G-1109A, Request for Approval to Accept Award and/or Gift From Outside Sources

The Office of Human Capital and Training (HCT) will use Form G-1109A to screen organizations and employees for potential conflicts of interest in the solicitation of external awards from non-Federal entities. This is to ensure the solicitations are not from for-profit businesses, contractors, or any entity that could benefit financially from DHS. In order to effectively screen and clear any USCIS award nomination from a non-Federal entity award program, HCT must collect information about the award, entity, underwriters, and the employee being nominated for the award. (April 25, 2018)

USCIS Minority Serving Institutions (MSI) Map

The Federal government recognizes MSIs as valuable resources to the nation. MSIs are institutions of higher education that serve minority populations. These include Historically Black Colleges and Universities, Hispanic Serving Institutions, Tribal Colleges and Universities, Asian Americans and Native American Pacific Islander Serving Institutions, and Predominantly Black Institutions. USCIS supports MSIs in the form of grants, services, and computer equipment donations. The MSI Map is an interactive map of the United States showing all MSIs and USCIS offices for the USCIS Office of Equal Opportunity and Inclusion. The MSI map has a searching capability of all domestic MSIs and the business contact information of points of contact at the MSI. (April 25, 2018)

U.S. Secret Service (USSS):

USSS 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. (November 29, 2007)