Privacy Impact Assessment
for the

Department of Homeland Security

Web Portals

DHS/ALL/PIA-015

June 15, 2009

<u>Contact Point</u>
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

Many Department of Homeland Security (DHS) operations and projects require collaboration and communication amongst affected stakeholders including employees, contractors, federal, state, local and tribal officials, as well as members of the public. One method of effectuating such collaboration is the establishment of an online "portal" allowing authorized users to obtain, post and exchange information, access common resources, and generally communicate with similarly situated and interested individuals. DHS has written this general privacy impact assessment (PIA) to document these informational and collaboration-based portals in operation at DHS and its components which collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or who seek to gain access to the portal "potential members."

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 these activities the Department requires 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 its partners involves the need to establish a means of communication that allows individuals from many different geographic regions to collaborate in a meaningful way. DHS and its components have created varying types of online portals designed to facilitate this collaboration. Most portals consist of the following elements or some combination thereof:

- Web-based interface
- User registration and authentication
- Log-in and verification
- General information area open to all users
- Specific subject matter areas open to select users
- Document libraries and common resources
- Collaboration tools such as a member directory, message boards, and/or shared spaces available for members to post comments, links and documents relevant to the subject of the portal.

DHS and its components' portals can be organized into two broad categories based on the overall purpose of the portal: 1) informational/collaboration-based, and 2) operations-based.

- **Informational/Collaboration-Based**– The primary purpose of this type of portal is to facilitate the dissemination and exchange of relevant information among authorized users. The content of the information exchanged through the portal does not contain PII except for limited contact information about portal members. Members of the portal may have the

ability to post relevant information such as lessons learned and best practices for the benefit of other members of the portal. PII collected from and exchanged among members is limited to contact information such as name, email address, and mailing address, and business or governmental affiliation. DHS also operates portals without collaboration tools that simply provide authorized users with access to information that do not contain PII. Such portals are for informational purposes only and collect PII solely for the purpose of facilitating registration to the portal. **This PIA covers informational/collaboration-based portals**.[1]

- **Operations-Based** –The primary purpose of this type of portal is to facilitate an operational function, mission, or process (e.g., law enforcement and intelligence, human resources, financial management, immigration processing, emergency management, etc). The content and exchange of information through this type of portal may contain PII (including sensitive PII) about individuals who are not members of the portal. For example, a law enforcement operations-based portal may be used to disseminate and exchange sensitive PII such as Social Security number, date of birth and a physical description about an individual who is the subject of an investigation. In this example, the purpose of the portal extends beyond a basic informational/collaborative scope. In addition, the information exchanged may include sensitive PII about a broader category of individuals that are not members of the portal. **This PIA does NOT cover operations-based portals**.

Portal operators seeking to determine whether their portal is informational or operational should answer the following questions:

- Do the portal's functions extend beyond informational and/or collaborative purposes into operational uses of PII?
- Does the portal collect or exchange sensitive PII?[2]
- Does the portal exchange PII about individuals that are not members or potential members of the portal?

Expanding the scope of collection beyond an informational/collaborative purpose, the collection and exchange of sensitive PII, and/or the exchange of PII about a broader category of individuals than members of the portal may create enhanced privacy risks. Accordingly, if a portal operator's answer to any of the above questions is yes, the portal in question is most likely an operations-based portal and will require a separate PIA.

Should a portal qualify as informational/collaboration-based, the operator may seek coverage by this DHS-wide PIA. In order to be considered as covered by this DHS-wide PIA, program managers and portal operators must submit a PTA to the DHS Privacy Office establishing that:

---

[1] Similar to the Contact Lists PIA used by DHS, portal operators seeking coverage by this general PIA must submit a specific Privacy Threshold Analysis to the Privacy Office.

[2] The Privacy Office encourages Components to collect non-sensitive PII as an alternative to sensitive PII wherever possible, including for registration purposes. If your Component seeks coverage by this PIA and collects sensitive PII for registration purposes, please consult with the Privacy Office and provide justification for the collection of this information. The Privacy Office will then determine whether the relevant portal may be covered by this PIA.

- A mission need for operation of the portal exists and the authority to collect the information lies within each program or project's authorizing legislation, regulation, or order.

- The portal members are verified during the registration process to ensure they are authorized to use the portal.[3]

- The information collected from and exchanged among portal members is limited to non-sensitive PII. A definition of sensitive PII can be found in the *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information*.[4]

- PII collected, used or exchanged is limited to the purpose(s) of facilitating registration to the portal, providing information to, and collaboration among authorized members.

- PII exchanged on the portal is limited to members' or potential members' contact information.

- Upon registration to the portal, an appropriate Privacy Act notice ((e)(3) statement) is given to the potential member outlining the uses of PII. Members are provided notice both at the time of registration and prior to posting any information that the purpose of the portal is for information and collaborative purposes and are instructed not to post operational PII on shared spaces of the portal. Portal administrators periodically review shared spaces to ensure PII is not posted and have the ability to remove inappropriate member postings.

- The portal has been reviewed by the Chief Information Security Officer (or designee) and if applicable, the portal has obtained an Authority to Operate (ATO) from the Chief Information Security Officer (or designee). [5]

- Applicable System of Records Notice(s) (SORNs) have been reviewed to ensure that the information collected and its uses do not exceed the boundaries of the notice (See Section 6).

Any program manager or portal operator seeking to use this PIA as privacy documentation for its portal must submit a specific PTA detailing how it has met these requirements to the Privacy Office. Please contact the Privacy Office to obtain this PTA at pia@dhs.gov or 703-235-0780. Once the PTA is approved and a determination is made that the portal meets the requirements, the portal's name and component will be added to Appendix A of this document as a qualifying portal.

---

[3] DHS operates multiple types of informational/collaboration based portals. Portal operators determine who is eligible to become a member of the portal and the level of verification of these individuals should be consummate with the risk of the informational/collaboration-based portal.
[4] DHS Privacy Office, *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security*, (Washington, D.C.: October 2008).
[5] Portal operators must provide the date of the ATO to the Privacy Office.

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?

Individuals seeking access to the portal provide limited contact information. This generally includes name, business affiliation, mailing address, phone number, and email address. As part of the registration process, individuals also supply answers to security questions in order to facilitate restoration of an account in the event of an expired or forgotten password. Security questions should not ask registrants to provide sensitive PII.

Upon successful registration to the portal, members voluntarily post information such as comments (e.g., lessons learned for emergency response), documents, or links (news articles, relevant resources). The content of the information posted does not contain PII other than associating the post with limited user contact information (e.g. posted by "Jane Doe"). Limited contact information about members may also be used to populate a member directory consistent with the collaboration purpose of the portal.

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

Information is collected directly from individuals seeking access to the portal. Individuals provide their information voluntarily. Individuals may also voluntarily post comments, links, and documents relevant to the portal subject matter. Members may not be the original source of information posted to shared spaces. For example a member may post links to relevant news articles or documents of which they are not the original author.

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

The information is collected to facilitate registration of authorized individuals to the portal, disseminate information regarding the Department's operations, and to facilitate collaboration among partners who are working with the Department on various projects.

1.4 How is the information collected?

Information is collected directly from members and potential members of the portal and 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. Members may have the ability to update their account information on the relevant portal. Information posted by authorized members to shared spaces on the portal is designed for collaborative

purposes only and is not verified for accuracy. Some portals may also provide members with the ability to update information posted by other authorized members though, ultimately, such updates are not verified for accuracy.

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 (e.g., statues, rules, regulations, treaties, orders) for this type of collection are established based on each component and each program's particular mission.

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 the operation of a web portal for informational and collaborative purposes is that more information will be collected than is necessary to distribute information or facilitate collaboration. In addition, since individuals may have the ability to post information to the portal, there is a risk that such postings could contain sensitive PII and/or PII that is not about members or potential members of the portal. To mitigate these risks, information collected from individuals is limited to specific contact information necessary to facilitate registration to the portal and collaboration among authorized members. Portal members may also have the ability to opt-out of a member directory or restrict access to certain contact information. To mitigate the risk of members posting PII to shared spaces, users are provided notice at the time of registration and prior to posting any information that specifically instructs them to ensure that their comments and documents do not contain PII outside the scope of contact information about members or potential members of the portal. Portal administrators periodically review shared spaces to ensure that PII is not posted and have the ability to remove inappropriate member postings.

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 facilitate registration of individuals seeking access to the relevant DHS portal. Upon registration, the use of PII facilitates the information and collaboration purposes of the portal. For example, the portal may use the limited contact information to create a member directory available to authorized users. Member activities such as to posting comments, links, and documents may be associated with their information such as a userid. Information may also be used consistent with the routine uses outlined in the System of Records Notices for the General Information Technology Access Account Records System (GITAARS) DHS/ALL-004, May 15, 2008, 73 FR 28139,

and the Department of Homeland Security Mailing and Other Lists System DHS/ALL-002, November 25, 2008, 73 FR 71659.

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

DHS informational/collaboration-based web portals do not use tools to analyze or manipulate PII.

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

Web portals covered under this PIA may use commercial or publicly available data that do not contain PII. For example, authorized members of the portal may post links or documents (e.g., news articles, best practice documents from an association) to shared spaces of the portal from commercial or publicly available sources. If web portal members routinely post commercial or publicly available data containing PII (e.g. to facilitate an operational function, mission, or process), it cannot be covered under this PIA.

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. This risk is primarily mitigated by collecting limited contact information about portal members and providing access to only authorized members of the portal. Members are verified during the registration process to ensure they are authorized to gain access to the applicable portal. DHS Portal operators determine what constitutes an authorized member. Members are further informed of appropriate uses of PII upon registration to the portal as well as through applicable system records notices such as the General Information Technology Access Account Records System (GITAARS) DHS/ALL-004, May 15, 2008, 73 FR 28139, and Department of Homeland Security (DHS) Mailing and Other Lists System DHS/ALL-002, November 25, 2008, 73 FR 71659. Additionally, all Department employees and contractors are trained on the appropriate use of PII further ensuring that those responsible for administering and operating the portal use PII appropriately.

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 only as long as it is useful for carrying out the information dissemination and/or collaboration purposes for which it was originally collected. Records

associated with DHS Web portals may be subject to different retention schedules depending on the type of information. As discussed in Section 1.0, DHS informational/collaboration-based portals collect information to 1) facilitate registration to the portal, 2) facilitate communication and collaboration among portal members (e.g. member directory), and 3) permit member activities such as posting information, comments, documents, and relevant links.

- Information collected to facilitate registration and access to the portal is retained per the requirements of General Records Schedule 24, section 6, "User Identification, Profiles, Authorizations, and Password Files." Inactive records will be destroyed or deleted 6 years after the user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.

- The limited contact information collected to facilitate communication and collaboration among portal members may be retained for up to three years or less depending on the record. For records that may be used in litigation, the files related to that litigation will be retained for three years after final court adjudication."

- Web portal operators along with records retention officers, determine an appropriate records schedule and retention period for information posted by its members.

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

Yes. Records pertaining to account access to the portal are retained and disposed of in accordance with the National Archives and Records Administration's General Records Schedule 24, section 6, "User Identification, Profiles, Authorizations, and Password Files."

Records pertaining to any contact lists or collaborative purposes are retained and disposed of in accordance with the National Archives and Records Administration's General Records Schedule 12 (Communications Records) or General Records Schedule 1.

Records pertaining to member activities such as posting documents, links, and articles will be retained in accordance with the component Web portal operator's approved records schedule.

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

Retaining PII for longer than as is relevant and necessary can introduce privacy risks such as unauthorized use or disclosure of PII. To mitigate the risk of retention of PII associated with the maintenance of the portal, individuals who no longer wish to participate in the online community may log-on or contact the portal operator to request removal of their account. DHS will then terminate the

account[6] and no longer retain the member's limited contact information, thereby reducing privacy risks posed by retention of their contact information. In addition, DHS has established approved records schedules for system of records that may apply to its portals that appropriately balance the need to retain the information against privacy risks.

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?

Information may be shared with internal DHS components inasmuch as they are involved in facilitating access to the portal, distributing information, or collaborating with partners within the Department. Generally, contact information supplied by members is not shared for any purpose beyond which it was originally collected. As noted in relevant DHS SORNs DHS/ALL-002 and DHS/ALL-004 and consistent with the requirements of the Privacy Act, information may be shared internally within DHS to those who demonstrate a need-to-know for the information for the official performance of their duties. For example, if the portal resides on a DHS network, DHS officials with a need-to-know are permitted to use the portal information to fulfill their official responsibilities for IT and counterterrorism purposes.

4.2 How is the information transmitted or disclosed?

Information may shared by electronic or paper means.

4.3 <u>Privacy Impact Analysis</u>: 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 PII. Department employees and contractors are trained on the appropriate use and sharing of PII. Further, any sharing of information must align with the purpose of the initial collection as well as any applicable SORNs.

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.

---

[6] DHS will terminate the account at the user's request; however records pertaining to account access are retained in accordance with General Records Schedule 24, Section 6, "User Identifications, Profiles, Authorizations, and Password Files."

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

Information may be shared with external governmental entities inasmuch as those entities are involved in distributing information or collaborating with partners within the Department. Generally, contact information is not shared for any purpose beyond which it was originally collected. Sharing with external entities is limited to the uses described in applicable SORNs DHS/ALL-002, and DHS/ALL-004.

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. The Department limits sharing of the PII to authorized members of the portal who may be a DHS partner at the state or local level, or a member of the public for collaborative purposes. Uses of the limited information are identified in the DHS/ALL-002 (November 25, 2008, 73 FR 71659) and DHS/ALL-004 (May 15, 2008, 73 FR 28139) SORNs and the notice provided when information is collected though the portal. Uses of the limited information beyond the purposes for which it was originally collected are not acceptable.

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

Information is shared outside the Department with members of the portal who may be a partner at the state or local level, or a member of the public through the applicable portal. Information shared with members of the portal is safeguarded by providing access controls so that only authorized members may access the portals resources.

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

A risk is presented whenever the Department shares information outside the Department that the information will be used beyond the purposes for which it was originally collected. Since members of the portal may be outside of the Department the exchange of information on the portal is considered to be external sharing. To mitigate the risks against uses of information beyond the purposes for which it was originally collected DHS employs access controls so that only authorized members may access the portals resources. Further, DHS informs portal members upon registration and through applicable SORNs about the appropriate uses and exchange of PII on the portal thus mitigating risks against inappropriate external sharing.

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. Specifically during the registration process users are provided with notice as to the collection and use of their information. Individuals are notified that certain contact information such as a userid may be associated with any postings to shared spaces on the portal. In addition, this PIA and the System of Records Notices for DHS/ALL-002 and DHS/ALL-004 provide notice regarding the collection of contact information by the Department.

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

Yes. Individuals are not required to provide their information. However, if individuals do not provide their information, they may not be able to obtain an account to access the relevant portal.

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

Depending on the portal, individuals may have the ability to consent to particular uses of the information. Specifically, informational/collaboration based portals that publish a member directory may permit individuals to opt-out of or limit the information published. DHS will use the information only for the purposes for which it was collected (e.g., facilitating registration to the portal, collaboration among members, contacting members) and identifies uses in its notices including this PIA and the System of Records Notices for DHS/ALL-002 and DHS/ALL-004. Should an individual suspect information is being used beyond the given scope of the collection; they are encouraged to either contact the Component Privacy Officer or write to the system managers listed at http://www.dhs.gov/foia under "contacts."

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.

Individuals voluntarily register to become a member of the portal in order to collaborate and exchange information with other members; thus individuals are well aware of the purpose for the collection. In addition, notice is provided to the user regarding the uses of their information upon registering to the portal. This PIA provides further notice to individuals as do the System of Records Notices DHS/All-002 and DHS/All-004.

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?

Individuals seeking access to their information may either log on to the relevant web portal or contact the portal owner to review their account information. Should an individual seek to remove their information from a portal they may either log on the relevant portal or contact the portal operator to gain access to, remove, or edit their information.

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

Generally, individuals may log on directly to the relevant web portal to correct any inaccurate information about them or update their contact information (e.g. e-mail address, phone number). If the individual cannot directly correct their record, the program or project that initially collected the information for operation of the portal is in the best position to correct any inaccurate information. Any inquires for correction should be made to the initial collector. Access requests can also be made through the DHS Freedom of Information Act (FOIA)/Privacy Act process. Instructions for filing a request may be found at http://www.dhs.gov/foia.

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 uses their contact information. Any risks associated with redress are thoroughly mitigated by the individual's ability to update or delete their information either directly by accessing the portal or by contacting the portal operator.

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?

Portal operators determine who is eligible to become a member of the portal. Potential members are verified during the registration process to ensure they are authorized to use the portal. Upon successful completion of the registration process, users may access the portal and its relevant resources (e.g. shared spaces, member directory). In terms of administration of the portal, 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 DHS employees and contractors 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 the portal supports. Many times contractors are tasked with either development or administration of the portal. Contractors are required to have the same level of security clearance as all other DHS employees in order to access Department computers.

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 PII such as what is contained in portals.

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

Portal owners seeking coverage by this PIA must be able to demonstrate that the portal is covered by a Certification and Accreditation (C&A) pursuant to the review processes established by the Chief Information Security Officer. In some cases, the portal may be supported by a larger information technology system subject to the requirements of the C&A process. In these cases, the information technology system supporting the portal must undergo the C&A process. Portal owners seeking coverage by this PIA should submit documentation to the Privacy Office demonstrating that an Authority to Operate (ATO) is in place for the applicable portal or IT system supporting the portal.

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. Authorized users must supply a valid log-on and password to obtain access to the portal.

Within DHS, access to portal resources and member information is limited to those who require it for completion of their official duties. Portal administrators periodically review shared spaces to ensure that postings by its members do not contain sensitive PII or PII about those who are not members or potential members of the online community. Administrators have the ability to remove any inappropriate postings.

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?

To mitigate risks against authorized access or use of PII, DHS implements access controls and limits the collection of PII to a limited set of contact information used to facilitate collaboration among authorized members of the portal. Access to the portal by Department employees and contractors is limited to those who have a need to know for the performance of their official duties. Further, the Department conducts thorough background checks on every employee and contractor. All Department employees and contractors are trained on privacy and security policies and procedures, specifically as they relate to PII.

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 information/collaboration based portals 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?

This PIA applies to all existing and planned collaboration/information-based portals. Administrators for existing portals are required to submit a PTA to ensure that privacy is addressed. For planned portals, a PTA is required before the portal becomes operational.

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

No technology used here raises specific privacy concerns. Portal members have the ability to post comments, links and documents but the content of these postings should not contain sensitive PII. Portal members are instructed specifically not to post PII to shared spaces. In addition, portal administrators periodically review shared spaces to ensure that PII is not posted and have the ability to remove inappropriate member postings.

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix: Systems Covered by the Web Portals PIA

Department of Homeland Security Interactive Portal

Department of Homeland Security Online

Federal Emergency Management Agency Debris Removal Contractor Registry (DRCR)

Federal Emergency Management Agency Integrated Security and Access Control (ISAAC)

Federal Emergency Management Agency Lessons Learned Information Sharing (LLIS)

Federal Emergency Management Agency Responder Knowledge Base

Federal Emergency Management Agency Secure Portal

Federal Emergency Management Agency State Preparedness Report Survey Tool

Federal Emergency Management Agency The Full-Spectrum Risk Knowledgebase

Federal Emergency Management Agency Universal Adversary Portal

Federal Emergency Management Agency Preparedness Compliance Assessment System Tool (PrepCAST)

National Protections and Programs Directorate 2010 Olympics Integrated Communications Plan

National Protections and Programs Directorate Constellation/Automated Critical Asset Management System

National Protections and Programs Directorate Infrastructure Risk Analysis Partnership Program (IRAPP)

National Protections and Programs Directorate Linking Encrypted Network System

National Protections and Programs Directorate TRIPwire

National Protections and Programs Directorate US-CERT Homeland Security Information Network Portal

Office of Health Affairs BioWatch Web Portal

Science and Technology CyberFETCH System

Science and Technology DisasterHelp.gov Web Portal

Science and Technology Homeland Open Security Technology (HOST)

Science and Technology External S&T Collaboration Site (E-STCS)

Science and Technology Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT)

Science and Technology BioDefense Knowledge Management System

Science and Technology First Responder Communities of Practice

Science and Technology Safety Act Management System (SAMS)

Science and Technology Tech Solutions

Science and Technology This week in Science and Technology (TWIST) Registration

Transportation and Security Administration Transportation Security Information Sharing and Analysis Center

Transportation Security Administration Automated Multi-Level Training Assessment Program/Quality Assurance Compliance Program

Transportation Security Administration Exercise Information System (EXIS)

Transportation Security Administration Passenger Fee Portal and Service System