Privacy Impact Assessment
for the

Stakeholder Engagement Initiative: Customer Relationship Management

December 10, 2009

Contact Point
Christine Campigotto
Private Sector Office
Policy
202-612-1623

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Office of the White House Liaison and the Office of Policy, in coordination with the Office of Intergovernmental Affairs, are developing the Customer Relationship Management (CRM), a data management tool being employed by the Stakeholder Engagement Initiative (SEI). The system will be an online database which manages information on external stakeholders and tracks the interactions between these individuals and DHS. This PIA is being conducted because personally identifiable information (PII) will be collected and maintained on a variety of stakeholders.

Overview

The Office of the White House Liaison and the Office of Policy, in coordination with the Office of Intergovernmental Affairs, are developing a system to track contact information and relationships with external stakeholders across the Department to avoid redundancy of effort and identify gaps in outreach efforts. This fulfills two expressed priorities of the Secretary of Homeland Security: efficiency and a unified DHS.

The system will store contact information on stakeholders such as the organization they work for, position within that organization, work phone numbers, and email address. It will track the issues in which those stakeholders have engaged and expressed interest, the interactions the stakeholder has had with DHS such as conversations with DHS employees, and attendance at DHS-affiliated events.

The system is designed to share information for the purpose of coordination. Access to this information will be restricted to those offices with the most direct relationship with any given stakeholder. The information that is shared is done so with the intent of harmonizing engagement.

A typical transaction may be as follows: The Assistant Secretary of Immigration and Customs Enforcement (ICE) speaks at a conference in Texas. After the conference, he converses with several attendees and receives their business cards. The information on those business cards is input into the system, marking them as stakeholders with a relationship with ICE. The next month, DHS is rolling out new guidance on worksite enforcement procedures. The Private Sector office (PSO) is instructed to identify stakeholders affected and ensure communication of the guidance to them. By running a search in the system, PSO can find the stakeholders that have previously engaged with DHS on this issue. PSO may also find that ICE has a long-standing relationship with one of those stakeholders. Rather than reach out directly, PSO will coordinate with ICE to ensure that ICE is communicating the relevant information to the individual. PSO may also find that while ICE has a strong representation of stakeholders in Texas, we are missing several key players in New Mexico. PSO can then direct their outreach efforts to forming new relationships in New Mexico, while trusting that ICE is leveraging their pre-existing relationships in Texas.

In another possible transaction, an employee of Google meets a PSO employee at a conference. That PSO employee entered their information, provided on a business card, into the database for storage and utilization. Months later, the Google employee is contacted by phone by a different PSO employee about an issue they initially flagged for interest. However, the Google employee has since switched jobs and is no longer interested in this issue. They request that they no longer be contacted by DHS. The contacting PSO employee sees on their record that the record is owned by the original PSO employee. They inform the original PSO employee of this, and the original PSO employee (the record owner) deletes the

Google employee's information from the system completely. While this particular example uses phone as the medium of requesting removal from the system, any medium is acceptable: in person or via phone, email, letter, etc.

Legislation defining the role of the Department requires that it engage and communicate with general public, private sector, and state, local, tribal, territorial, and international government. The January 2007 Report of the Culture Task Force, from the Homeland Security Advisory Committee (HSAC), states in Recommendation 5 that

> "one of the roles of the DHS headquarters should be to establish regionalization requirements for the component organizations, designed to clarify and facilitate their coordination with state and local authorities…to eliminate component gaps, conflicts, or overlaps…to optimize the capabilities of DHS headquarters and take advantage of the component organizations' relationships with the state, local, tribal and private sector."

This system is thus intended to facilitate meeting DHS's statutory requirements, as well as HSAC recommendations.

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?

The information tracked falls in to five types:

1. **Organizations**: Information on the organizations with which DHS engages is tracked: Organization name, address, office phone, issues on which the organization engages, and DHS groups in which the organization may participate (e.g. a task force).
2. **Individuals**: Information on individual points of contact is tracked: Salutation, first and last name, title, personal phone numbers, email address, work address, issues on which the individual engages, and various generic interests of the individual (e.g., that this individual uses social media regularly, or that this individual often writes op-eds for a local newspaper). Additionally, there will be a notes field for any user to provide comments to expand the DHS knowledge base of the individual. The notes field may include such information as non-DHS events that the stakeholder attended, or relationships they have with other stakeholders. (This information is provided to DHS by the respective stakeholder through the regular course of conversation.) The notes field will not be used to document attributes such as race, ethnicity, or religion.

   Information on conversations and interactions DHS has with stakeholders may be tracked: Date and mode of communication (e.g. phone call, email), the component

and individual at DHS that had the conversation, and any relevant outcomes of the conversation (e.g., a promise to follow up), which would be for added transparency and situational awareness. The CRM will show the most recent timestamp in the contact history section.

3. **Events**: Information on meetings and events on which DHS has collaborated is tracked: Name and date of the event, agenda of the event, issues discussed at the event, and attendees of the event.

4. **Issues**: Information on issues that are important to the stakeholder aligned to the Secretary's five priorities (Immigration, Secure Borders, Disaster Response, Counterterrorism, and OneDHS) will be tracked in the CRM. Recent events regarding the issue, recent updates to policy, talking points, and documents relevant to the issue may be uploaded.

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

DHS employees generate the information in the system by working with stakeholders who voluntarily provide their information to DHS staff, for outreach and communication purposes. Currently, this information exists in inconsistent formats throughout the DHS, from excel spreadsheets to offline databases to the contacts portion within Outlook. CRM will provide for standardization of contact information and ensure that relationships are maintained regardless of personnel change.

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

This information is being collected and used to fulfill two of Secretary Napolitano's priorities:

First, efficiency: With the ability to see the information that exists across DHS and the work that is being done by a variety of offices, each individual on the system will be able to best utilize their time avoiding redundant work and targeting the areas which are identified as needing to be prioritized.

Second, a unified DHS: The dissemination of this information across the department allows offices to act within the context of what DHS is doing as a whole. Conversations can be couched with a historical understanding of what other components have done, and stakeholders will be engaged consistently and strategically.

1.4 How is the information collected?

DHS employees input the data as they have conversations with the stakeholders. In the case where there is not a preexisting relationship with a particular organization, DHS employees may perform a public search for an organization and enter the address and contact information into the system. DHS may then reach out to the organization for external stakeholder outreach purposes such as to extend an invitation to a DHS event or function.

1.5 How will the information be checked for accuracy?

There is not a systematic process for verifying the information; however, all users have the ability to delete or update almost all fields in the database, enabling the immediate correction of inaccurate information, as needed. In addition, an audit trail is kept for system access and all transactions that request, create, update, or delete information from the system. The audit trail/log, which includes the date, time, and user for each transaction, is secured from unauthorized modification, access, or destruction.

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

The Homeland Security Act of 2002, Public Law 107-296, Title I, Section 102(c) [6 U.S.C. § 112(c)] defines the functions of the Secretary of Homeland Security to include engagement and communication with the private sector and state, local, tribal, territorial, and international government:

(c) COORDINATION WITH NON-FEDERAL ENTITIES.—With respect to homeland security, the Secretary shall coordinate through the Office of State and Local Coordination (established under section 801) (including the provision of training and equipment) with State and local government personnel, agencies, and authorities, with the private sector, and with other entities, including by -

(1) coordinating with State and local government personnel, agencies, and authorities, and with the private sector, to ensure adequate planning, equipment, training, and exercise activities;

(2) coordinating and, as appropriate, consolidating, the Federal Government's communications and systems of communications relating to homeland security with State and local government personnel, agencies, and authorities, the private sector, other entities, and the public; and

(3) distributing or, as appropriate, coordinating the distribution of, warnings and information to State and local government personnel, agencies, and authorities and to the public.

Further, the January 2007 Report of the Culture Task Force, from HSAC, states in Recommendation 5:

"one of the roles of the DHS headquarters should be to establish regionalization requirements for the component organizations, designed to clarify and facilitate their coordination with state and local authorities…to eliminate component gaps, conflicts, or overlaps…to optimize the capabilities of DHS headquarters and take advantage of the component organizations' relationships with the state, local, tribal and private sector."

This system is thus intended to facilitate meeting DHS's statutory requirements, as well as fulfilling HSAC recommendations.

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

The primary risk of collection in CRM will be that more PII than necessary or inappropriate PII, such as race or religion, may be captured in the open notes field. To mitigate this risk, all users will be required to attend privacy training specifically tailored to this system, and there will be regular review and monitoring of the types of information captured within CRM.

Further, All DHS employees and contractors are required to follow DHS Management Directive (MD) Number: 11042, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, May 11, 2004. This guidance controls the manner in which DHS employees and contractors must handle Sensitive but Unclassified/For Official Use Only Information. All employees and contractors are required to follow Rules of Behavior contained in the DHS Sensitive Systems Handbook. Additionally, all DHS employees are required to take annual computer security training, which includes training on appropriate use of sensitive data and proper security measures.

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 information is used primarily to inform DHS conversations with external stakeholders. The contact information is used to communicate with the stakeholder, and the issue and interaction information is used to better define those conversations to be most effective.

Additionally, the information may be used in aggregate for a broader, strategic view of stakeholder engagement occurring at DHS. It may identify spots of redundancy, or gaps in DHS efforts, enabling resources to be directed most efficiently.

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

All data analysis is housed within the system. Reports on outreach activity may be run periodically to address the broader use of the information outlined above. A report on how many stakeholders in a given region DHS has spoken to about a particular issue, for example, may illustrate if more or less resources need to be allocated for that outreach; or a report on how many stakeholders have been identified within a FEMA region may illustrate that our contacts are unevenly distributed throughout the country and need to be established in a neglected region.

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

The system tracks only the information listed in Section 1.1 for any given stakeholder. If that information is publicly available, it may be inputted in to the system. For example, if the address of a Senator's office is on her website, that address may be input in the database under that Senator's contact information.

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.

There is a privacy risk that information may be used inconsistently with the purpose stated within this PIA. To mitigate this risk, at the start of each CRM session all participating users are required to affirmatively acknowledge the following responsibilities regarding the use and dissemination of CRM records:

- Information may be used only for DHS outreach purposes.
- Any unauthorized access may be subject to criminal and civil penalties;
- Each participating agency is responsible for its own compliance in collecting, maintaining, and sharing information under the Privacy Act and any applicable regulations.

Further, these risks will be mitigated by logging and auditing of the event logs on a weekly basis by the Information System Security Officer (ISSO).

Section 3.0 Retention

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

3.1 What information is retained?

All information outlined in Section 1.1 of this PIA is retained in the system.

3.2 How long is information retained?

The system contains reference material that can be updated or deleted when no longer needed for business use. The business rules will state that if a stakeholder has not been contacted within one year, or a particular policy issue is no longer active or relevant, the data will be deleted at that time.

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

The data in the system is reference material, also known as "non-record." As such, according to NARA, we do not need an approved schedule for the system.

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

There is a risk that CRM data could be maintained for a period longer than necessary to achieve the underlying mission. Although there is always risk inherent in retaining reference material for any length of time, the business rules that will be communicated to users involving the deleting of irrelevant data are consistent with the concept of retaining reference material only for as long as necessary to support the agency's mission. NARA has agreed by indicating retention schedule approval is not necessary for this system.

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?

Currently, the following offices will be using the system:

- Front Office, Scheduling, White House Liaison Office
- Policy: Homeland Security Advisory Council, Private Sector Office, State and Local Law Enforcement, Screening Coordination Office, Policy Development
- Intergovernmental Affairs
- Office of Legislative Affairs
- Federal Emergency Management Association
- U.S. Citizenship and Immigration Services
- Immigration and Customs Enforcement
- Customs and Border Protection
- Civil Rights and Civil Liberties
- Privacy Office
- Office of Public Affairs
- Gulf Coast Recovery Office

Information shared across all participating components and offices is: the names of the organizations and individual points of contact, the issues which they engage in, organizations' addresses, events participated in, and interactions with the stakeholder. Information NOT shared with all offices and components, and limited by user access rights and roles, is cell phone numbers and email addresses of individuals.

4.2 How is the information transmitted or disclosed?

The information is all housed in the system to which all participating components have access.

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.

The primary risks associated with internal sharing is unauthorized disclosure and potential misuse of the data by authorized users. To mitigate these risks, access to the system is limited to authorized users. Within the system, all users are limited in the data they can see and/or manipulate by both the Component to which they belong, and the access level which they are set to. DHS policies and procedures are in place to limit the use of and access to all data in CRM to the purposes for which it was collected. Computer security concerns are minimized by the fact that the information shared internally remains within the DHS environment. An audit trail is kept for system access and all transactions that request, create, update, or delete information from the system. The audit trail/log, which includes the date, time, and user for each transaction, is secured from unauthorized modification, access, or destruction.

These risks will be further mitigated by tailored Rules of Behavior and security awareness training for users of SEI.

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?

This information is not routinely shared outside DHS, but if it is, this sharing will be consistent with DHS/ALL-002 Mailing and Other List System SORN (69 FR 70460).

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.

This information is not routinely shared outside DHS, but if it is, this sharing will be consistent with DHS/ALL-002 Mailing and Other List System SORN (69 FR 70460).

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

This information is not routinely shared outside DHS, but if it is, this sharing will be consistent with DHS/ALL-002 Mailing and Other List System SORN (69 FR 70460).

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

This information is not routinely shared outside DHS, but if it is, this sharing will be consistent with DHS/ALL-002 Mailing and Other List System SORN (69 FR 70460).

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?

Much of the information collected is provided directly by the stakeholder; all other information is public information. Individuals are provided general notice through the DHS Mailing List and Other List System, DHS/ALL-002, system of records notice (SORN) published in the Federal Register at 69 FR 70460, as well as through this PIA.

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

Yes, stakeholders may notify DHS employees that they will not make their contact information available.

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

The information in the system is used to initiate and maintain contact with the given stakeholder. At any point, the individual may request to no longer be contacted by DHS. When such a request is made, information will be deleted from the database by the 'owner' of that stakeholder's data.

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.

Notice is provided through this PIA and the DHS/ALL-002 SORN. Additionally, through the primary use of the information, users of the system will be in contact with the individuals, who at any point in those conversations may express their desire to have their information used, or not used, in a certain manner. When such a request is made, DHS will immediately comply.

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 may provide correct information to the system users, who may input it on their record.

In addition, individuals may gain access to their own information by submitting a Privacy Act (PA)/Freedom of Information Act (FOIA) request. Instruction for filing a request may be found at http://www.dhs.gov/foia.

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

All users are permitted to update individuals' information within the system and may do so as correct information is provided.

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

Stakeholders will be notified by phone/email when DHS employees are verifying that they have the current contact information for the individual or organization. Any changes will be updated in the system, including requests to no longer be contacted.

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

The individual may request at any time that their information be changed or removed through the system. This request may be made through any medium (phone, in writing, or in person).

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

The privacy risk associated with redress is that individuals will not have access and ability to correct their information. In this instance, this risk is minimal in that DHS employees contact stakeholders via phone/email to verify accuracy of information regarding the individual. Any changes are updated in the system by authorized users.

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?

Access to the system is linked to employees' DHSNet accounts – as such, users may access the system only with an account on the DHS network. Users must have a purchased license designated for their use, and must be approved by their office administrator, who are in turn approved by the system owners and/or administrators.

The users are documented within the system, which has user management capabilities. Access to the application will be audited via the event logs of the application.

8.2 Will Department contractors have access to the system?

If Department contractors have accounts on the DHS network, they will have access to the system if deemed relevant to their job description.

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

Rules of Behavior and Standards Operating Procedures will be disseminated to all users to the system, which will include information on privacy guidelines and the usage of the system. All users are required to attend annual security awareness training.

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

The system used to host this application will reside on a server that is currently C&A at the HIGH security categorization and hosts other similar Microsoft applications such as SharePoint. The application will inherit the management, operational, and technical controls of this system.

CRM will be treated as a minor application, which has not had a formal C&A. Being a minor application, the process will be greatly streamlined as most of the controls will be inherited from the major application, MOSS 2007. C&A has been completed for MOSS 2007 with an Authority to Operate dated January 23, 2009.

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

The ability to export sensitive information is being disabled for all non-administrative users of the system. The primary risks for CRM are loss of confidentiality from internal sources and potential misuse of the data by authorized users. These risks will be mitigated by event logging and auditing of the event logs on a weekly basis by the ISSO.

Additionally, firewalls are being set up between components so that personal information shared with an employee in one component cannot be viewed by employees of other components.

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 primary risks for CRM are loss of confidentiality from internal sources and potential misuse of the data by authorized users. These risks will be mitigated by tailored Rules of Behavior and security awareness training for users of SEI and weekly audit log review by the ISSO.

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?

The system is a customized off-the-shelf Customer Relationship Management (CRM) system.

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

The system is currently in the design stage. The project development lifecycle used was Systems Engineering Lifecycle (SELC).

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

The technology itself is only designed to hold the data inputted by Department staff. As such, business use of the technology may raise privacy concerns, outlined throughout this PIA, but the technology itself does not.

Responsible Officials

Christine Campigotto

Private Sector Office

Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security