Privacy Impact Assessment
for the

GovDelivery Email Subscription Management System

March 7, 2008

Contact Point
Tina Kelley
Internet Services Office
E-Gov Services Staff
202-616-0992

Reviewing Official
Vance Hitch, Chief Information Officer
Department of Justice/Office of the Chief Information Officer
(202) 514-0507

Approving Official
Kenneth Mortensen, Acting Chief Privacy Officer
and Civil Liberties Officer
Department of Justice
(202) 353-8878

Introduction

The GovDelivery Email Subscription Management System ("GovDelivery ESM" or the "System") is a web-based software system invented, owned, and operated by GovDelivery, Inc. of St. Paul, MN. The system is used to handle email and digital subscription management and to deliver opt-in email and other messaging. GovDelivery ESM is hosted at GovDelivery, Inc.'s Tier III data center and delivered on a Software as a Service (SaaS) basis to nearly 250 public entities including, among others, the U.S. Department of Homeland Security, Labor, Treasury, Transportation, and the Federal Reserve. The System allows website visitors of agency clients to subscribe to receive email and wireless alerts based on individual, self-selected, needs and interests.

Section 1.0
The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

The only personally identifiable information collected are email addresses. The system also collects information on which web pages people wish to receive notifications about when those web pages are updated. The DOJ webpage from which the GovDelivery page starts will collect certain information, as all DOJ web page interactions do, including IP address, pages accessed, pages requested, and time and date of access. A full list of the information collected is located on the DOJ Web Privacy Policy page.

1.2 From whom is the information collected?

Visitors to the Department of Justice's public websites who voluntarily subscribe to the service.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

Email addresses are collected so subscribers can be notified by email when a web page of interest to them has been updated.

Section 3.0
Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

The email addresses are used only to send email messages to subscribers alerting them that new or updated content has been posted on the website. The email alerts relate to selected sections of the website that subscribers have identified as being of interest to them.

Section 4.0
Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

Each DOJ Office or Component that establishes a separate account with GovDelivery will have to designate a DOJ employee as the account administrator. The account administrator will have access only to the email address of individuals who subscribe to receive update notifications concerning their Component web pages. The account administrator will be advised about privacy issues and will be required to complete a certification regarding the proper handling of the subscribers' email addresses.

Section 5.0
External Sharing and Disclosure

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

5.1 With which external (non-DOJ) recipient(s) is the information shared?

GovDelivery, DOJ's contractor for this service receives the email addresses directly from the subscriber. A notice will inform users that they are leaving a DOJ website. A discussion of the security and access controls used by GovDelivery.com is included in Section 8.

Section 6.0 Notice

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

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Yes. Before an individual subscribes to the GovDelivery service, he is presented with a web page which details exactly how his information will be handled by GovDelivery, Inc. and by the Department. Links are provided to the privacy policies of both GovDelivery, Inc. and the Department. In addition, a link to the Department's Systems of Records notice, as published in the Federal Register, is included on the web page and in the Privacy Act notice when the email address is collected from the individual.

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

Yes, individuals may choose not to subscribe simply by choosing not to fill out the subscription form and clicking on the cancel button. Subscribers may unsubscribe at any time, by clicking on a link to their profile, which is provided with every email. The profile details which web pages the individual subscribes to and offers check boxes to unsubscribe to specific pages and/or to delete their subscription to the service. When an individual unsubscribes, his email address is permanently deleted. A full backup of the system is run early every morning and incremental backups every 5 minutes during the day, so any database activity (such as a profile deletion) is almost immediately incorporated in the backup structure. Backups are kept for 1 year.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Individuals can control how their email addresses are used by deciding whether or not to sign up for the service, and then by choosing what updates they wish to receive and how often they receive them. Subscribers can also modify their email addresses at any time or unsubscribe from the service.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Because a Privacy Act notice is included on the website as well as links to both the Department's and GovDelivery, Inc.'s privacy policies and to the Department's System of Records Notices that cover the collection of information, the risk that an individual would not be providing his email without knowledgeable consent is mitigated. The various notices provide the individual with transparency concerning the Department's collection, use, and maintenance of the related information.

Section 7.0
Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

All email alerts include links to the subscriber's User Profile. Clicking on the link opens a new browser with the profile. Subscribers can review and modify their information in their profile at any time. Subscribers are also provided with an email address where questions or problems can be sent.

To minimize the risk that an individual might incorrectly enter his email address, a second confirmation email address entry is required during the subscription process.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

Before individuals subscribe to the service, an introductory web page presents information about subscribing and changing and deleting information. In addition, all email alerts include a link to the subscriber's User Profile.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

If the system is inoperative, the subscriber can contact either GovDelivery, Inc. or DOJ. Every email update contains a standard footer with contact information for both GovDelivery and DOJ.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

Because the individual can update or modify his email address stored in the system, the risk of the Department holding inaccurate information about an individual is mitigated.

Section 8.0
Technical Access and Security

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

8.1 Which user group(s) will have access to the system?

Four user groups have access to the GovDelivery ESM and the data contained therein.

1. End Users (also known as subscribers). End users access GovDelivery ESM via links placed on client web pages or in system-generated emails. GovDelivery ESM subscribers have access to their own personal data and the information made public by the GovDelivery's clients.
2. DOJ Administrators. There are five client DOJ administrator roles, each with varying degrees of permissions and system access. DOJ administrators have web-based, password controlled access to data pertaining to their account. Most DOJ administrator interactions are for one the following purposes:
    - send email bulletin to subscribers
    - add new subscription item (web page) to system
    - upload content to system including individual email addresses or mailing lists

3. GovDelivery, Inc. Administrators. There are 2 classes of GovDelivery, Inc. administrator. GovDelivery, Inc. administrators have web-based, password controlled access to data from one or more client implementations. Most GovDelivery, Inc. administrator interactions are for one of the following purposes:
    - set up a new client in the system
    - view report data
    - assist client administrators with implementation support
4. GovDelivery, Inc. Technical Staff. GovDelivery system administrators have network access via certificate-based virtual private network (VPN) to GovDelivery ESM components (hardware and software) for the purpose of maintaining and monitoring the system. Additionally, GovDelivery, Inc. has longstanding relationships with contractors whom they periodically call upon to assist with specific and specialized elements of the system. All contractor work is supervised by GovDelivery, Inc. employees and conducted from GovDelivery's office or hosting center.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Yes. GovDelivery, Inc. owns and operates GovDelivery ESM as a hosted, SaaS system at its St. Paul, MN data center. GovDelivery, Inc. administrators and technical staff have access to the system and data stored therein. Certain GovDelivery, Inc. sub-contractors will occasionally have supervised and limited access to the system for the purpose of executing specific and specialized technical operations. All GovDelivery, Inc. employees and contractors are bound to keep client data confidential.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. Please see the answer to Section 8.1.

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

GovDelivery, Inc.'s ESM administrators and technical staff are assigned roles based on their job function and are given only the permissions needed to perform their work. This determination is made by the GovDelivery Inc.'s Director of Technical Operations. This and other security procedures are documented in the GovDelivery Inc.'s security plan and procedures.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Each month a system administrator will review user accounts on the application, web servers, Oracle, and VPN certificates to ensure that each account and its permissions match the authorization roster.

Rules and permissions for roles are tested with each software release.

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

GovDelivery, Inc. logs, maintains, and audits as necessary application, network, server, and database activity. System activity is restricted by the use of session cookies, URL parameters, and form parameters.

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

All GovDelivery, Inc. ESM administrators and technical staff are briefed on data integrity and confidentiality concerns at hiring and periodically throughout employment. GovDelivery, Inc. users are subject to the GovDelivery, Inc.'s Rules of Behavior.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

GovDelivery, Inc. follows NIST guidelines in implementing and managing its security policies (NIST Publications 800-18, *Guide for Developing Security Plans for Information Technology Systems*, and 800-44, *Guidelines on Securing Public Web Servers*). Several agencies have reviewed GovDelivery, Inc. and System security documentation as recently as July 2007 (Department of Homeland Security reviewed the procedures at that time). In all cases, the security procedures and documentation were accepted by the agencies and the System was authorized for use. Further steps were deemed unnecessary by the reviewing agencies. This is largely due to three factors:

1. Execution of the contract to setup and use GovDelivery ESM does not require contractor access to government facilities.
2. There is no interconnection between GovDelivery ESM and government systems. GovDelivery accesses government websites via public ports (just like any visitor to a public government web page), and government administrators access GovDelivery ESM

through secure ports via standard web browsers over the Internet (just as they would access a bank account).

3. Government information stored on GovDelivery servers has not been deemed to be sensitive at a level requiring further review. Information stored on GovDelivery's servers includes a user's email address, subscription preferences (e.g., topics of interest), and perhaps a password and/or responses to government-initiated questions. While the designation of "sensitive information" is left to the discretion of each agency, the information stored in GovDelivery ESM has never been found to meet the requirements of "sensitive information" as defined by the Computer Security Act of 1987, Public Law 100-235:
    - "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy."

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

The security of our client and subscriber data is a priority for GovDelivery, Inc., and we endeavor to prevent unauthorized access to the System and the data contained therein. The Company has developed a comprehensive security plan that has been reviewed and approved by several federal executive agencies. The Company has never had a breach of its System or its data. Security controls include:

- The System infrastructure is hosted in a secure, Tier III data center that includes five levels of physical security.
- The System is protected by state of the art firewalls.
- The Company logs, maintains, and audits as necessary application, network, server, and database activity.
- Access to client data is limited to client and high-level GovDelivery, Inc. administrators and only to the extent needed to perform their duties.
- System activity is restricted by the use of session cookies, URL parameters, and form parameters.
- There is mandatory password protection of administrator accounts and optional password protection on subscriber accounts. Passwords are never sent or shown in the clear.
- Administrator sessions automatically time out after a configurable period of inactivity.

Conclusion

GovDelivery ESM was built and is still operated as a multi-tenant, SaaS platform. From the point of invention, the segregation, security, and integrity of client data in the System has been a

preeminent concern of the Company. As such, security considerations and risks are evaluated with all development and deployment activities, including but not limited to the release of new functionality, features, and platform infrastructure. The Company continuously monitors and evaluates new technologies and assesses the potential impact (positive or negative) on the System's security posture.

Responsible Officials

Tina Kelley

Internet Services Office

Department of Justice

Approval Signature Page

_____/s/_____March 7, 2008

Kenneth P. Mortensen
Acting Chief Privacy and Civil Liberties Officer
Department of Justice