U.S. Securities and Exchange Commission

GovDelivery Communications Cloud
PRIVACY IMPACT ASSESSMENT (PIA)

December 30, 2015

Office of Information Technology

Privacy Impact Assessment
GovDelivery Communications Cloud

Publishing History

Document Publication Number	Revision	Date	Changes Made
Initial Document	Initiation	07/29/09	Document Creation
Document update	1	12/29/15	Addition of the new (SMS) and Widget services, and changes in technology, including commercial cloud services
Document update	2		
Document update	3		
Document update	4		
Document update	5		
Document update	6		

General Information

1. Name of Project or System.
   GovDelivery Communications Cloud

2. Describe the project <u>and</u> its purpose or function in the SEC's IT environment.
   The GovDelivery Communications Cloud ("GovDelivery" 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. The system is hosted at GovDelivery, Inc.'s Tier III data centers and delivered on a Software-as-a-Service ("SaaS") basis to over 1,000 public entities including, among others, the U.S. Department of Homeland Security, Department of Labor, Department of the Treasury, Department of Transportation, Department of Justice, and the Federal Reserve. The System allows website visitors to subscribe to receive email and wireless alerts based on individual, self-selected, needs and interests.

   The Securities and Exchange Commission ("SEC") recently upgraded GovDelivery services to include direct SMS capability, which will improve delivery time and capacity for short message service ("SMS") delivery. In the past, the SEC's GovDelivery subscription only permitted the conversion of email to SMS, which delays SMS delivery. The SEC procured direct SMS capability where SMS delivery will not be delayed. Direct SMS also allows subscribers to send an inbound SMS message in order to sign themselves up for SMS or email notifications from the SEC. Furthermore, in the past, the SEC's GovDelivery contract did not include Widget capability whereby the Widget displays information in a way that a user can interact with the operating system and application (e.g., SEC.gov websites) to be able to download information from SEC.gov to other websites and also drive traffic to the SEC.gov. Widgets also permit individuals to sign up for GovDelivery alerts from the SEC.gov website. The current GovDelivery subscription provides for Widget capability. Additionally, the SEC's Office of Public Affairs ("OPA") procured upgraded GovDelivery services to enable the SEC staff to sign-up to receive email and SMS alerts from the SEC internal website (Intranet) on SEC approved devices.

   The purpose of the system is to handle digital subscription management and to deliver opt-in email and other messaging.

3. Requested Operational Date? Currently operational; however, OPA procured upgraded SMS and Widget services from GovDelivery on September 1, 2013. This PIA update reflects the addition of the new SMS and Widget services, and changes in technology, controls and collection of information.

4. System of Records Notice ("SORN") number? "Mailing, Contact and Other Lists" (SEC-56)

5. Is this an Exhibit 300 project or system? ☒ No □ Yes

6. What specific legal authorities, arrangements, and/or agreements allow the collection of this information? Delegation of Authority per 5 U.S.C. § 302.

Specific Questions

<u>SECTION I - Data in the System</u>

1. What data about individuals could be collected, generated, or retained?
   The system primarily collects email and SMS addresses. The system also collects information on which SEC.gov web pages people wish to receive notifications when those web pages are updated. The SEC web page from which the GovDelivery page starts will collect certain information, as all SEC web page interactions do, including IP address, pages accessed, pages requested, and time and date of access.

   Email messages sent are also tracked to understand the open and engagement rate of the messaging. This information correlates only to the subscription address and allows the SEC to understand the impact of messaging in terms of effectiveness of the content based on engagement of the recipients.

2. Does the project/system use or collect the social security number ("SSN")? (This includes truncated SSNs)
   ☒ No. □ Yes. If yes, provide the function of the SSN and the legal authority to collect.

3. What are the sources of the data?
   The data originates from visitors who voluntarily subscribe to the service.

4. Why is the data being collected?
   The data is being collected to subscribe visitors to a delivery opt-in email and SMS system and to understand the effectiveness of the SEC's communications.

5. What technologies will be used to collect the data?
   All GovDelivery solutions are cloud-based and are provided on a SaaS basis. All GovDelivery applications are hosted in Tier III data centers on GovDelivery's secure infrastructure, eliminating hardware or software installation and investments, ultimately reducing costs for the SEC.

SECTION II - Attributes of the Data (use and accuracy)

1. Describe the uses of the data.
   The email addresses are used only to send email, SMS and Widget messages to subscribers, alerting them that new or updated content has been posted on SEC websites. The email, SMS, and Widget alerts are related to selected sections of the SEC websites that subscribers have identified as being of interest to them.

   The open and click through data is used to understand the effectiveness of messaging and the SEC's communications efforts. This data can be used to inform the SEC of popular content and messaging for future publication consideration.
2. Does the system analyze data to assist users in identifying previously unknown areas of note, concern or pattern? ☒ No □ Yes If yes, please explain:

3. How will the data collected from individuals or derived by the system be checked for accuracy?
   The system requires the user to input his email or SMS address twice, but the data is not checked for accuracy; if a subscriber provides an incorrect email address, the system automatically generates an undeliverable notification.

SECTION III - Sharing Practices

1. Will the data be shared with any internal organizations?
   ☒ No □ Yes If yes, please list organization(s):
   OPA staff will be the account administrator. The account administrator will have access only to the email addresses of individuals who subscribe to receive update notifications concerning their selected SEC.gov 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.

2. Will the data be shared with any external organizations?
   ☒ No □ Yes If yes, please list organizations(s): How is the data transmitted or disclosed to external organization(s)?

3. How is the shared data secured by external recipients?
   Data is never shared outside of GovDelivery's Cloud. Email addresses are entered into the system directly from the subscriber. A notice will inform users that they are using an SEC approved external system with a link to the SEC's privacy policy. A discussion of the security and access controls used by GovDelivery.com is included in Section V.

4. Does the project/system process or access PII in any other SEC system?
   ☒ No
   □ Yes. If yes, list system(s).

SECTION IV - Notice to Individuals to Decline/Consent Use

1. What privacy notice was provided to the different individuals prior to collection of data? (Check all that apply)
   □ Privacy Act Statement □ System of Records Notice ☒ Privacy Impact Assessment
   ☒ Web Privacy Policy □ Notice was not provided to individuals prior to collection
   Before an individual subscribes to the GovDelivery service, he is presented with a web page that details how his information will be handled by GovDelivery, Inc. and by the SEC with a link to the SEC.gov's Privacy Policy.

2. Do individuals have the opportunity and/or right to decline to provide data?
   ☒ Yes □ No □ N/A
   Please explain: Yes, individuals may choose not to subscribe simply by choosing not to fill out the subscription form or by clicking on the cancel button prior to submitting the form. Subscribers may unsubscribe at any time, by clicking on a link to their profile, which is provided with every GovDelivery email. They may also reply STOP to any SMS message to discontinue SMS subscription. The profile details which web pages the individual subscribes to and offers check boxes to unsubscribe to specific pages and/or to delete their entire subscription to this service. When an individual unsubscribes, his subscription is permanently deleted.

3. Do individuals have the right to consent to particular uses of the data?
   ☒ Yes □ No □ N/A
   Please explain: Individuals can control how their subscription 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.

SECTION V - Access to Data (administrative and technological controls)

1. Has the retention schedule been established by the National Archives and Records Administration ("NARA")?
   ☒ No If no, please explain: The SEC's Office of Records Management Services ("ORMS") confirmed that the "page watch" alerts and RSS feeds are not considered federal records. If the GovDelivery system is used to send unique emails with Commission generated content, then there may be unique records created for which OPA will coordinate with ORMS to determine NARA recordkeeping responsibilities. Currently, such usage of GovDelivery is not expected to be usual.

   □ Yes If yes, list retention period:

2. Describe the privacy training provided to users, either generally or specifically relevant to the program or system?
   All SEC employees and Contractors with access to this system receive Privacy and Security Training that outlines their responsibilities for protecting and securing personally identifiable information. All GovDelivery, Inc. administrators and technical staff are briefed on data integrity and confidentiality concerns at hiring and periodically throughout employment. Under their SEC contract, GovDelivery, Inc. users are subject to the GovDelivery, Inc.'s Rules of Behavior. Further, GovDelivery plans and procedures are outlined in question 3, below.

3. Has a system security plan been completed for the information system(s) supporting the project?
   □ Yes If yes, please provide date SA&A was completed:
   ☒ No If the project does not trigger the SA&A requirement, state that along with an explanation: The SEC reviewed security assessment and authorization (SA&A) documentation completed by the National Institute of Standards and Technology (NIST), which was determined, at the time, to sufficiently document the required security controls.

   GovDelivery, Inc. owns and operates the GovDelivery Communications Cloud as a hosted, SaaS system at its two data centers. 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 and have executed non-disclosure agreements.

   The GovDelivery Communications Cloud is a service offering that has Federal Information Security Management Act ("FISMA") compliant assessment and authorization (A&A) package and has received an Authority to Operate to process federal data. The A&A package consists of a:

   - Configuration Management Plan
   - Privacy Impact Assessment
   - Contingency Plan
   - Contingency Plan Test
   - Incident Response Plan
   - Rules of Behavior
   - System Security Plan
   - Security Controls Assessment

- Plan of Action and Milestones

GovDelivery and its services are purposely built for government. GovDelivery's core solution, the Communications Cloud, allows public sector organizations to develop and manage digital communications, specifically: email communications, social media channels, and SMS/text messaging. There are currently over 1,000 clients using GovDelivery including federal and state entities, state governments, cities and townships, and European governments.

NIST conducted an independent security review of GovDelivery's policies, products, and infrastructure and is typically willing to share their findings directly with other government entities.

GovDelivery's services undergo an annual certification and accreditation audit by NIST in which they review GovDelivery's Security Plan, Continuity of Operations Plan and Threat and Risk Assessments.

The SEC was able to examine some of the NIST GovDelivery assessments.

GovDelivery is in the process of going through the Federal Risk and Authorization Management Program (FedRAMP) and obtaining a provisional authorization from the Joint Authorization Board, consisting of the General Services Administration and the Departments of Homeland Security and Defense. https://www.fedramp.gov/marketplace/in-process-systems/govdelivery-govdelivery-communications-cloud/

4. Is the system exposed to the Internet without going through a virtual private network ("VPN")?
☒ No
☐ Yes If yes, Is secure authentication required? ☐No ☐Yes; and
Is the session encrypted? ☐ No ☐Yes

5. Are there regular (i.e. periodic, recurring, etc.) PII data extractions from the system?
☒ No
☐ Yes If yes, please explain:

6. Which user group(s) will have access to the system?
GovDelivery contractors will have access to the system. Also, four user groups have access to the GovDelivery system and the data contained therein.

1. End Users (also known as subscribers). End users access the GovDelivery system via links placed on client web pages or in system-generated emails. GovDelivery subscribers have access to their own personal data and the information made public by GovDelivery's clients.

2. SEC Administrators. There are four client SEC administrator roles, each with varying degrees of permissions and system access. All four clients may not be used. The SEC can control and assign which internal staff members or designated SEC Contractors (i.e. related to the web redesign) should be GovDelivery administrators and grant the appropriate level of access. SEC administrators have web-based, password controlled access to data pertaining to their account. Most SEC 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 list.

3. GovDelivery, Inc. Administrators. 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 a VPN to GovDelivery 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.

7. How is access to the data by a user determined?
Access is determined on a need-to-know basis and is provided to users by administrators and technical staff. Procedures are documented in operating procedures.

Are procedures documented? ☒ Yes □ No

8. How are the actual assignments of roles and rules verified?
SEC administrator login activity is fully reviewable by SEC administrators at any time.

9. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) 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.

SECTION VI - Privacy Analysis

Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

There is a very low potential for privacy risks. The PII collected consists of the individual's email and SMS addresses. Individuals are given multiple ways to opt-out of receiving communications. Subscribers may unsubscribe at any time, by clicking on a link to their profile, which is provided with every GovDelivery email. Individuals may also reply STOP to any SMS message to discontinue SMS subscription. When an individual unsubscribes, the individual's subscription is permanently deleted from the GovDelivery system.

Also, GovDelivery has implemented security policies and procedures in accordance with National Institute of Standards and Technology (NIST) guidelines. The security of client and subscriber data is a priority for GovDelivery, Inc., and they endeavor to prevent unauthorized access to the System and the data contained therein. The Company has developed a comprehensive security plan, which is being independently assessed through FedRAMP. As part of GovDelivery's security process, a risk assessment is conducted annually. In addition, GovDelivery conducts regular penetration tests with an independent assessor and performs their own security scans on a monthly basis to ensure that data remains private.