



## Special Inspector General for Afghanistan Reconstruction

Main: 703-602-2500  
2530 Crystal Drive  
Arlington, VA 22202-3934  
[www.sigar.mil](http://www.sigar.mil)

# PRIVACY IMPACT ASSESSMENT

## INTRODUCTION

This Privacy Impact Analysis (PIA) is conducted pursuant to Section 208 of the E-Government Act of 2002 (Public Law 107-347), and is used to determine the scope, justification, and appropriateness of use of information technology that collects, maintains, or disseminates information in identifiable form, also referred to as personally identifiable information (PII).

<b>Directorate or Component:</b>	<b>Communications &amp; Congressional Relations (CCR)</b>
<b>System Name:</b>	<b>SIGAR Third-party Social Media Services</b>
<b>System Acronym:</b>	<b>N/A</b>
<b>System Owner:</b>	<b>SIGAR Communications &amp; Congressional Relations Directorate</b>

### A. Information and Privacy

To fulfill the Special Inspector General for Afghanistan Reconstruction's (SIGAR) legal obligations to protect PII, SIGAR systems must meet the following requirements:

- Use of the information must be controlled.
- Information may be used only for necessary and lawful purposes.
- Information collected for a particular purpose must not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.
- Information collected must be sufficiently accurate, relevant, timely, and complete to ensure the individual's privacy rights.

**B. Contact Information:**

1. Who is the person completing this PIA?

Name: Philip J. LaVelle  
Title: Director of Public Affairs  
Component: CCR  
Address: 2530 Crystal Drive, Arlington, VA 22202-3934

2. Who is the System Manager for this system or application?

Name: Philip J. LaVelle  
Title: Director of Public Affairs  
Component: CCR  
Address: 2530 Crystal Drive, Arlington, VA 22202-3934  
Telephone number: (703) 545-5974

3. Who is the IT Security Manager for this system or application?

Name: Roland Wong  
Title: IT Director  
Component: Information Management Office, Management and Support  
Address: 1550 Crystal Drive, Suite 9000, Arlington, VA 22202

4. Who is the Chief Privacy Officer or designee who reviewed this document?

Name: Hugo Teufel  
Title: Director, Privacy, Records & Disclosure  
Component: OGC/PRD  
Address: 1550 Crystal Drive, Suite 9000, Arlington, VA 22202

## C. System Description

This section of the PIA describes the application and the method used to collect, process, and store information. Additionally, it includes information about the business functions the system supports.

SIGAR uses Twitter, a third-party website located at [www.twitter.com](http://www.twitter.com), to disseminate information to the public. Additionally, SIGAR in the future may expand its social media presence to include Facebook, YouTube and other third-party social web services. These applications allow for enhanced information sharing by enabling communication between many users. SIGAR uses Twitter, and may use other services in the future, to improve the agency's ability to communicate mission-related information to the public, to increase transparency, and to promote public participation. Twitter, and the other social media services that SIGAR may use in the future, are not part of the agency's or the Federal government's internal information systems and will not be operated by agency contractors.

Third-party postings on SIGAR's social media account(s) are under the dominion of third-party social websites. Information collected and stored by the social media applications is subject to the third party privacy policies posted on their website. SIGAR does not and will not collect information from individuals when they interact with the agency's social web accounts. In addition, SIGAR does not collect, maintain or disseminate information provided by individuals to social websites. Any information other users provide to register on third-party websites, or that they post in response to SIGAR posts, is provided voluntarily and is not maintained by SIGAR.

## D. Data in the System

1. What personal information about individuals or other information that can personally identify an individual (name, social security number, date of birth, address, etc.) is contained in the system? Explain.

This system may contain information passed through a social media site to facilitate interaction with SIGAR such as, but not limited to: first name, last name, username, e-mail address, home or work address, contact information, and phone numbers. It may also include input and feedback from the public, such as comments, e-mails, videos, and other images with may include tag, geotags or geographic metadata.

SIGAR does not collect, maintain or disseminate PII from individuals who interact with third-party social websites that the agency uses. SIGAR does not collect, maintain or disseminate this information. Additionally, SIGAR does not collect, maintain or disseminate personal information from individuals who interact with SIGAR's accounts.

2. Can individuals “opt-out” by declining to provide personal information or by consenting only to a particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies)?

Yes Explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data): Twitter users and other third-party social-media website users are subject to the security and privacy policies of the site in question, and must consent to the website’s collection and use of information, such as name, username, password and email address, in order to register and use the service. Additional information collected may include picture, biography, location coordinates, IP address, and metadata associated with tweets. Users can control access to personal information and location information through account settings. SIGAR does not control privacy policy of Twitter or other social-media websites, use of information or content of tweets, and does not request, collect, maintain or disseminate personal information from Twitter or other social-media websites.

No Explain:

3. What are the sources of the information in the system? How are they derived? Explain.

SIGAR disseminates information and provides updates on various agency matters, to include audits, inspections, investigations, job openings and the HOTLINE. The information posted on third-party social-media websites is also available on the SIGAR website. Sources of information available to SIGAR are third-party social-media website users, including members of the public and federal employees, who post comments and profile information on the official SIGAR page on third-party social-media websites.

4. What Federal agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

Federal agencies may utilize third-party social-media websites to enhance communication or disseminate information; however SIGAR does not receive PII or other data from federal agencies through use of social-media websites.

5. What state and local agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

State and local agencies may utilize social-media websites to disseminate information and enhance communication; however, SIGAR does not

receive PII or other information from these agencies through the use of social-media websites.

6. What other third party sources will be providing data to the system? Explain the data that will be provided, the purpose for it, and how will it be used.

None.

#### **E. Access to Data:**

1. Who will have access to the data in the system (e.g., users, managers, system administrators, developers, contractors, other)? Explain their purpose for having access to this information.

SIGAR has the same access to data in social-media websites as other social-media website users, such as the general public, federal employees, private organizations and federal, state and local agencies. SIGAR has no control over user account settings or content posted to social-media websites, and does not collect, maintain or disseminate PII from use of social-media websites. Social-media users are subject to the social website's privacy policy for collection and use of information, and may set their account settings to limit access to personal information.

2. How is access to the data determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Explain the process.

Access to data is determined by social-media website privacy policy and user account settings, both of which are governed and controlled by the social-media website. SIGAR has no control over access restrictions, account settings, policy on collection and use of information, or security controls.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.
4. Social-media website users can set their account settings to control access to their personal information. SIGAR has no authority or control over access restrictions, account settings, user information, social-media website privacy policy or security controls. SIGAR only has control over official information posted on SIGAR's official social-media page. What controls are in place to prevent the misuse (e.g., browsing) of data by those having access? (Please list processes and training materials) Explain the controls that have been established and how are they monitored or reviewed.

Social-media website users can set account settings to control access to their personal information, and are subject to social-media website privacy policy on collection and use of personal information. SIGAR has no control over access restrictions, account settings, user information, social-media website privacy policy or security controls.

5. Do other systems share data or have access to the data in the system? If yes, explain the purpose for the need to have access.

No.

6. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface? Has policy or procedures been established for this responsibility and accountability? Explain.

Social-media website users are subject to social-media website security and privacy policies, and must consent to the website's collection and use of information; SIGAR does not control social-media website privacy policy, and does not request, collect, maintain or disseminate personal information from social-media websites.

7. If other agencies use the data, how will the data be used? Who establishes the criteria for what data can be shared? Have non-disclosure agreements been effected? Explain the purpose for the need to share the data?

SIGAR does not collect or maintain PII from use of social-media websites. Official information posted by SIGAR on social-media websites is reviewed and approved for public dissemination prior to posting.

8. Who is responsible for assuring proper use of the data? Is this individual fully accountable should the integrity of the data be compromised? Explain.

Social-media website users are subject to social-media website security and privacy policies, and must consent to the website's collection and use of information; SIGAR does not control social-media website privacy policy, and does not request, collect, maintain or disseminate personal information from social-media websites.

9. Explain the magnitude of harm to SIGAR if privacy related data is disclosed, intentionally or unintentionally. Would the reputation of SIGAR be affected?

N/A

10. What involvement will a contractor have with the design and maintenance of the system? Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been developed for contractors who work on the system?

Social-media websites are third-party independently operated software as a service application. SIGAR does not have a part in the development or maintenance of social-media websites.

11. Explain whether or not the data owner is contacted if it is not clear if other agencies share or have access to the data.

N/A

#### **F. Accuracy, Timeliness, and Reliability**

1. How is the data collected from sources other than SIGAR records verified? Has action been taken to determine its reliability that it is virus free and does not contain malicious code? Who is responsible for this making this determination? Explain.

SIGAR does not collect or maintain PII from use of social-media websites and does not verify data. Official information posted by SIGAR on social-media websites is reviewed and approved for public dissemination prior to posting.

2. How will data be checked for completeness? How is this being measured? What is the source for ensuring the completeness of the data? Explain the method used.

SIGAR does not check data posted by other users on social-media websites for completeness. Official mission-related information posted on social-media websites is reviewed and approved for public dissemination prior to posting.

#### **G. Attributes of the Data?**

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? Is this part of the system design? Is this documented, if so, where is the document located? Explain.

SIGAR does not collect or maintain data on individuals. Information and comments provided may be utilized by SIGAR to facilitate interaction with the public, to disseminate information regarding an upcoming event, to notify the public of an emergency or breaking news, or solicit feedback

about SIGAR's programs. SIGAR may also respond to information received directly from individuals who provide feedback from social media outreach using alternate methods, such as an e-mail directly to SIGAR.

2. Will the system derive personal identifiable information from any new data previously non-inclusive, about an individual through aggregation from the information collected? What steps are taken to make this determination? Explain.

No. SIGAR does not collect, maintain or disseminate data about individuals from the use of social-media websites.

3. Can the system make privacy determinations about employees that would not be possible without the new data? If so, explain.

SIGAR does not collect, maintain or disseminate data on individuals from use of social-media websites.

4. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Does the consolidation of data result in personal identifiable information? Explain.

No data is being consolidated.

5. How is the data retrieved? Can it be retrieved by a personal identifier (e.g., social security number)? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

SIGAR does not retrieve data on individuals using social-media websites.

6. What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them? Explain how they are distributed.

SIGAR does not generate reports on individuals from use of social-media websites.

#### **H. Maintenance and Administrative Controls:**

1. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites? Will the same controls be used? Explain.



N/A

2. What are the retention periods of data in this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines? Explain.

SIGAR does not collect, maintain or disseminate PII from use of social-media websites. Records are retained and disposed of in accordance with SIGAR social media proposed records schedule. The disposition is temporary, and records will be destroyed when no longer needed for agency business.

3. What are the procedures for disposition of the data at the end of the retention period? How long will any reports produced be maintained? Where are the procedures documented? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the procedures? Explain.

The data will be removed from the system and degaussed. The owner of the system will document the destruction through the agency's Electronic Records Management System.

4. Is the system using technologies in ways that SIGAR has not previously employed (e.g., Monitoring software, SmartCards, Caller-ID, biometrics, PIV cards, etc.)? Explain.

N/A

5. How does the use of this technology affect privacy? Does the use of this technology introduce compromise that did not exist prior to the deployment of this technology? Explain.

SIGAR use of social-media websites has a minimal affect on privacy, as SIGAR does not collect, maintain or disseminate any PII from social-media websites. SIGAR does not have any control over personal information posted by individual social-media website users. Social-media website users are subject to social-media website privacy policy and terms of use, and can set their account settings to protect their personal information.

6. If monitoring is being performed, describe the data being collected. Is monitoring required? If so, describe the need for the monitoring and identify the requirements and explain how the information is protected.

N/A

7. If monitoring is not required, explain the controls that will be used to prevent unauthorized monitoring?

N/A

8. In the Federal Register, under which Privacy Act Systems of Record (SOR) does this system operate? Provide number and name.

N/A

9. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

N/A

#### **I. Business Processes and Technology**

1. Does the conduct of this PIA result in circumstances that requires changes to business processes?

No.


2. Does the completion of this PIA potentially result in technology changes?

No.

**Privacy Impact Assessment  
Authorization Memorandum**

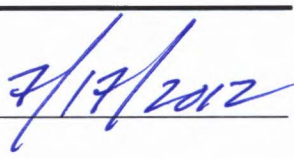
**This system or application was assessed and its Privacy Impact Assessment approved for publication.**

---



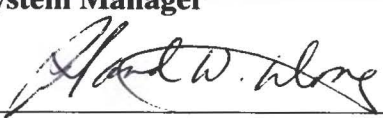
---

**System Manager**



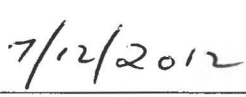
---

**Date**



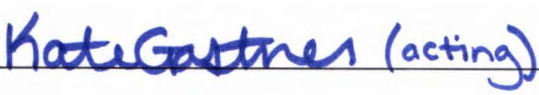
---

**Information Technology Security Manager**



---

**Date**



---

**Chief Privacy Officer**



---

**Date**