Special Inspector General for Afghanistan Reconstruction
Main: 703-602-2500
2530 Crystal Drive
Arlington, VA 22202-3934
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).

Directorate or Component:	**Management and Support**
System Name:	**Mr. FixIT**
System Acronym:	**Mr. FixIT**
System Owner:	**Burt Glassman**

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:	Burt Glassman
Title:	Purchasing Agent
Organization:	SIGAR
Contact Information:	
Address:	1550 Crystal Drive, Suite 9000; Arlington VA 22202
Telephone number:	7035456023

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

Name:	Burt Glassman
Title:	Purchasing Agent
Organization:	SIGAR
Address:	1550 Crystal Drive, Suite 9000; Arlington VA 22202

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

Name:	
Title:	
Organization:	
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
Organization:	Office of General Counsel
Address:	1550 Crystal Drive, Suite 9000; Arlington VA 22202

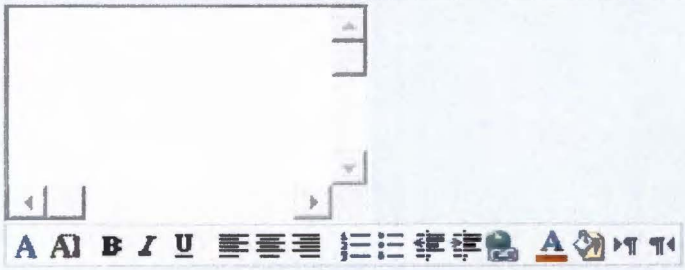
C. System Description

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.

Mr. FixIT is a single-point customer service portal that allows users to submit service requests, also known as "tickets". Tickets may be for one of the following service areas:

- Facilities
- Security
- Supplies
- Transportation
- Training
- IT/PC/Telephone
- Web Updates

It also provides administrative information detailing the quantity and quality of service requests and their eventual disposition. The system allows Management and Support to better provide customer service and support to agency employees. The system was built in and is managed in SharePoint. Below is a sample of the interface:

Issue Title *	
Service *	..Chose Service Select the service area from drop down box.(Required field)
Issue	 Select the issue from drop down and double click on the issue.
Description	 To paste text in this field: Move the cursor to the Description field and on the keyboard press CTRL + V (i.e. Control and Letter V at the same time) or Shift + Insert shortcut keys. Note: Right Click in the Description field will not display the copy & paste options.
Floor Number	Floor 9 Please select your floor number
Your Directorate *	
Attach File	No Yes Feel Free to attach a photo if it will help to describe your issue. Click the "Attach File" option on the top left of this form above the Issue Title.
Requestor	 Fill this field only if you are creating this ticket on the behalf of another person. If this request is for yourself you don't have to fill this field.
Title	For Admin Us The ticket number will be automatically generated in this field. Any updates to this field will be overwritten.

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.

   Name, email address, floor. Other information contained in the Department of Defense (DOD) Global Address List (GAL), which provides the system information at the time of login. Information contained in the system is that of the user and any SIGAR personnel assigned to respond to the ticket. Management and Support staff are the sole-users of the back-end portion of the system.

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):

   X No Explain: Login is DOD Common Access Card (CAC) driven. No further PII is requested.

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

   The user, using pull-down menus and fields, inputs information into the system, addressing the service areas, addressed above.

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.

   Other than information from SIGAR and SIGAR employees, the only other information is DOD – CAC-driven verification.

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.

   N/A

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.

   N/A

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.

   Users-Their own submission data.
   Managers-All submission data related to their respective area of service (Facilities, IT etc.).
   Techs-submission data related to tickets assigned to them.
   Administrators- All submission data.

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 system is specific to the support being provided by the respective M&S provider. Access is approved by system manager who is currently the system owner. Before access to the system is provided, the respective M&S manager, security for example, would notify the system manager of the need to add someone to Mr. FixIT to conduct actions in the system.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

   Restricted by level of responsibility. See E.1 Further, users always have access to their prior tickets, to include tickets not started, tickets in progress, and tickets completed.

4. 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.

   All activities are logged by intranet-based SharePoint back-end system and attributed to CAC signee like access to any other SIGAR Intranet-based file system.

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.

   The system manager is responsible for protecting the privacy rights of individuals. A training manual has been developed and distributed to users.

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?

   No other agencies will use the data.

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.

   The system manager is fully accountable for the service information contained in the system.

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

   In most cases, there is minimal harm to the agency if privacy related data is disclosed, intentionally or unintentionally, because the PII is not sensitive (name, work phone number). Harm is minimal because the nature of the requests made in Mr. FixIT are service related and are generally not personal. Beyond information contained in the DOD-Wide GAL there is no further information which could harm the agency as a whole.

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?

    Mr. FixIT was developed technically by a contractor name Syed Hasan, who is currently on contract through the end of the fiscal year FY12. He is directly responsible for the day-to-day operations and maintenance of the Mr. FixIT system. The contractor signed a confidentiality agreement upon the start of employment with SIGAR.

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.

No other agencies have access to the data.

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.

   No external data is collected.

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.

   N/A

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.

   The data is relevant and necessary to address the concerns of the employee and to identify the employee who has the issue to be fixed. Without the name of the employee we would not be able to remedy the problem.

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.

   N/A

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

   N/A

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 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.

   Data is received based on their CAC sign-in to SIGAR's PCs. As a user logs-in to a PC at SIGAR they are verified by their CAC certificate which identifies them according to the data entered at the time of their CAC provisioning. When a ticket is submitted in Mr. FixIT, the login information providing by the CAC essentially stamps the Mr. FixIT ticket so M&S staff knows who has a problem to fix.

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.

   The only reports that can be created by Mr. FixIT related to individuals are reports that detail who has submitted what ticket and what issues they have. The tickets will be used by M&S staff to remedy any issues they might have shared with M&S. Mr. FixIT administrators and Mr. FixIT managers/technicians (relative to their respective areas) will have access to these reports. These reports are not distributed, but instead generated and updated continuously on the Mr. FixIT SharePoint site.

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.

   Operated on one site. SIGAR's Intranet SharePoint portal.

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.

   The information stored in Mr. Fix-It is covered by the General Records Schedule. The General Records Schedules are issued by the Archivist of the United States to provide disposition authorization for records common to several or all of the agencies of the Federal Government. All general records schedule items are temporary, and should be deleted and destroyed according to their disposition schedule.

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 according to the data's retention schedule and degaussed. Any paper records generated from the system will be shredded. The owner for the system will document the destruction of data through the agency's Electronic Records Management System.

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

   No.

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.

   No.

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.

   Monitoring of the quantity and quality of service concerns is being performed. Monitoring allows for assurance that staff facilities, IT, supply, transportation etc. service is being provided in a timely and professional manner.

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

   Required to ensure service is timely and of quality.

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

   SIGAR-12, Internal Electronic Collaboration Tools

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

   No.

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** 9/23/12
Information Technology Security Manager	**Date** 7/26/12
Chief Privacy Officer (acting)	**Date** 7/23/2012