



# The OGIS Access System (OAS) Privacy Impact Assessment

## **Table of Contents**

Section I. Introduction and Overview.....	page 3
Section II. The Information in the System.....	page 5
Section III: Intended Use of Information.....	page 7
Section IV: Sharing of Collected Information.....	page 8
Section V: Opportunities for Individuals to Decline Providing Information.....	page 10
Section VI: Security of Collected Information.....	page 11
Section VII: System of Records Covered by the Privacy Act.....	page 13
Appendix A: NARA 40: Privacy Act System of Record Notice.....	page 14

## Section I. Introduction and Overview

### 1.1 Introduction

This Privacy Impact Assessment documents the types of personal information protected under the Privacy Act (PA) and the Freedom of Information Act (FOIA) that the OGIS Access System (OAS) processes and stores. In addition, this document identifies the categories of individuals to whom this information pertains, and the system controls that will be used to protect access to this information. OGIS will continue to revise this PIA as appropriate.

### 1.2 Purpose

This PIA addresses privacy issues raised by the use of OAS. It will also ensure that the collection and use of name-retrievable information in OAS is in compliance with applicable laws and regulations concerning personal privacy.

### 1.3 Terms and Definitions

1. Case: A request for OGIS assistance that warrants the opening of a file.
2. Case status: Information pertaining to the stage of a case within the OGIS process.
3. Customer: OGIS customers are members of the public and other Federal agencies.
4. Matter: A request for OGIS assistance that does not warrant the opening of a file. OGIS tracks the receipt of these requests for reporting purposes.
5. Mediation Services: The umbrella term “mediation services” includes the following: (1) mediation, a process in which a neutral third party, a mediator, assists disputing parties in reaching a mutually agreeable resolution; (2) facilitation, one approach used by mediators to assist each party to communicate and to understand the other’s position, interests, and needs; and (3) ombuds services, where an ombudsman acts as a confidential and informal information resource, communications channel, complaint-handler, and dispute-resolver.
6. Stakeholders: OGIS customers and mediators handling OGIS cases.
7. Users: OAS users are OGIS users and OGIS customers.

## I.4 OAS Overview

The OGIS Access System (OAS) is an information technology system that will be used to track and manage the various activities that are performed to manage OGIS programs and mediate disputes coming from members of the public or other Federal agencies. The system will encompass all hardware, software, communications capabilities, procedures, and documentation that is required for OGIS to mediate FOIA disputes and serve as the FOIA Ombudsman.

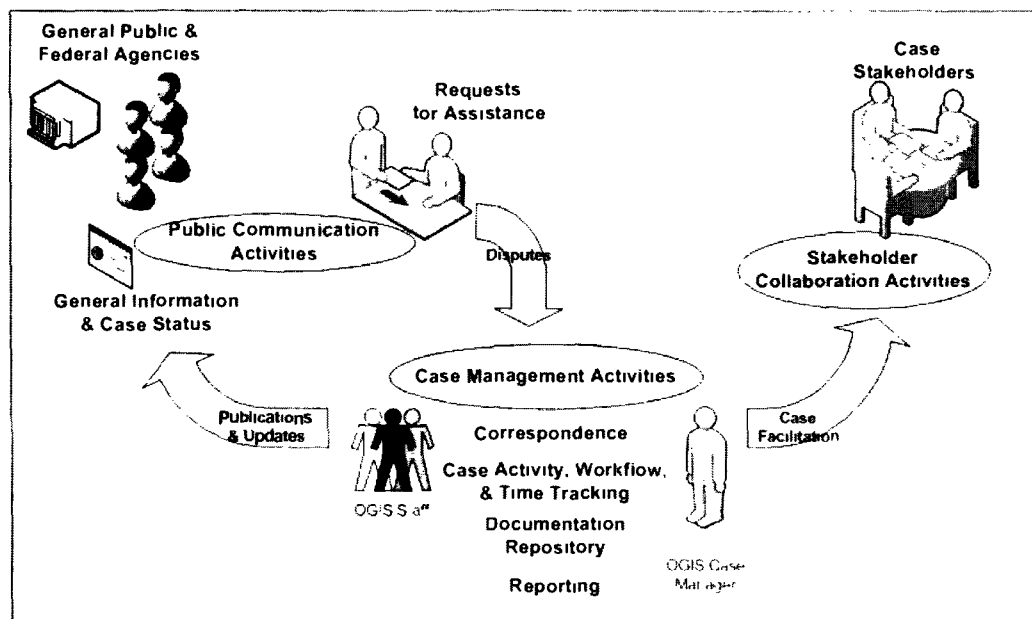
The OGIS has three main categories of business functions and activities requiring IT automation support that the OAS will be used to perform, as described below:

(1) *Case Management Activities* – These activities are foundational to OGIS’s business processes and enable the OGIS staff to: (a) record, track, and manage all information about cases and matters; (b) collect, manage, and secure documentation associated with cases and matters, (c) define, track, and manage workflow, (d) track staff time and effort, (e) generate and manage correspondence; (f) generate management metrics and reports, and (g) secure all information having PII ramifications. All new cases and matters can be received electronically through the OAS. OGIS can also receive new cases and matters through the U.S. mail, email or fax. OGIS staff will convert these cases and matters into electronic images and upload into the OAS.

(2) *Stakeholder Collaborative Activities* – These activities support collaboration on case matters and issues. Two types of collaborative activities are envisioned: (a) ad hoc collaboration that can be supported by general purpose web collaboration tools such as WIKIs, BLOGs, discussions boards and teleconferencing; and (b) formalized collaborative forums that are managed by case workers, restricted to specific stakeholders, and provide recorded transcripts of collaboration activities. These capabilities will be provided by commercially available web meeting and teleconferencing software or services.

(3) *Public Communication Activities* – These activities support OGIS communications with public stakeholders, mostly by publishing web accessible information. This information will include a knowledge base that will help guide the public in determining if OGIS can provide assistance. The information will also include OGIS-related training, web/video conference capabilities, Frequently Asked Questions, outside facing Blogs, case status information, contact information, relevant publications, and links to other relevant web sites. All of this information will be available through a web portal (proposed ogis.gov) that is accessible for public use, and will allow the submission of requests to OGIS for assistance.

Figure 1.4-1 Main Categories of Business Functions



The OAS is equipped with robust status accounting, work metric measurements, and management reporting capabilities.

## Section II. The Information in the System

### II.1 What data is in the system?

The OAS contains three general categories of information about individuals.

- Information about users of the system.
- Information about the customers that contact OGIS, which is inputted in the system either by the customers themselves or by OGIS personnel.
- Scanned materials consisting of request letters, administrative appeal letters, and correspondence between a requester and a Federal agency.

There are two different types of users:

- NARA (OGIS) employees who use the system in performance of their duties
- Any customer that uses the system to check the status of a case submitted to through the OAS to OGIS.
  - a. **What information will be collected from the customer?**  
All customers must provide contact information, including name (first and last) and home or business address, and may provide a telephone number, and email address. OGIS customers should also provide a description of what the customer wants OGIS to do for him/her: a statement of the nature of the dispute (such as

denial or delay); copies of all correspondence between the requester and agency; a list of the agencies involved; and a signed and dated customer authorization for OGIS to exchange information and records with other Federal agencies pertaining to the requester's FOIA and/or Privacy Act request/administrative appeal.

The customer can either input the information into the system through the web portal [www.ogis.gov](http://www.ogis.gov), or they can submit it via mail, fax or email and an authorized OGIS staff member will input the information, and scan documents, into the OAS. A paper case file will also be kept for one-year after the closure of a case file. These data elements are required for OGIS's business purposes based on the information needs that OGIS has observed in the past 20 months of operation. The Privacy Act of 1974 requires that OGIS obtain customers' prior written consent as stated above before OGIS can provide services to its customers.

When creating a case, a customer also has the option of creating a username and password to check the status of their cases. The username and password must be between 6-16 characters, include letters, numbers and special characters. The customer also has the ability to check the status of the case by using the access code that is given to the user once a case has been created.

**b. What information will be collected from NARA (OGIS) employees?**

Authorized OGIS users will have a unique username, password, and a third secured identifier (i.e., RSA token) to log-in to the OAS system, which will be on the NARAnet system. The username for OGIS users will be the unique username provided by NARA. The password is the same password used for accessing all NARA IT systems. Each user will have specific parameters for their rights and permissions to perform necessary OGIS duties. Specific data regarding the date and time actions are taken by a specific employee user will also be tracked and kept for auditing purposes. No other identifying information will be collected on employees.

**c. What information will be collected from other federal agencies?**

Federal agency personnel may provide background information regarding the request or appeal that is the subject of the case in the OAS. The requester's name, the agency's name, and contact information for agency personnel, and relevant information pertaining to the request or appeal will be kept in the OAS.

### Section III: Intended Use of Information

III.1: Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

The OAS will allow customers to create an account that lists all of the cases they have submitted to OGIS. The FOIA request(s) number(s) can also be associated with the individual. However, no new data will be created or derived about the individual.

III.2 Will the new data be placed in the individual's record?

The OAS will not create new data about OGIS customers.

III.3 Can the system make determinations about employees and /or the public that would not be possible without the new data?

Not applicable.

III.4 How will the new data be verified for relevance and accuracy?

Not applicable.

III.5 If the data is being consolidated, what controls are in place to protect data from unauthorized access or use.

Access to the OAS is granted in accordance with the permissions set by the system administrators and outlined in the Administrator Guidelines document (available upon request).

III. 6 How will the data be protected from unauthorized access?

The OAS contains protocols that will ensure that access is only granted to users within their set permissions. A management control grants access to specific users for certain parts of cases or matters. When a user no longer requires access to the system, the System Administrator will terminate the user's access rights.

III.7 How will data be retrieved by a user?

Based on the user type and the level of access granted, a user may be able to access the cases in which they are the case manager, the OGIS customer or have been granted access by the case manager or OGIS management.

III. 8 Is the data retrievable by a personal identifier?

Yes, data can be retrieved by a customer's name, OAS case number, or FOIA request or appeal number.

III.9 What kind of reports can be produced on individuals?

Reports can be generated to list the opened and closed cases in the database as well as the status of the cases.

III.10 Can the use of this system allow NARA to treat the public, employees, or other persons differently?

Yes, the OAS has the ability to treat each user differently. The public has the ability to create a username and password where they can have direct access to OAS and check the status of their cases. Employee users have similar access to OAS, plus the ability to change content in the case files. OGIS users will have different levels of access to OAS based on their job duties.

III. 11 Will this system be used to identify, locate, and monitor individuals?

No.

III. 12 What kinds of information are collected as a function of the monitoring of individuals?

Not applicable.

III. 13 What controls will be used to prevent unauthorized monitoring?

Not applicable.

III. 14 Does it use persistent cookies or other tracking devices to identify web visitors?

No.

III. 15 Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes, the OAS is being designed to manage OGIS's workload, to provide statistical reports concerning volume of cases and matters received and the performance of employees, and to provide information to the public about the FOIA process and OGIS's services.

#### Section IV: Sharing of Collected Information

IV. 1 Who will have access to the data in the system?

Managers of OGIS, users, system administrators, and the developer of the software will all have access to the data.



IV. 2 How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

The user type will determine the level of access allowed. Each system user will have specific limited permissions. OGIS management will grant access and direct the system administrator to make changes to allow access to individual users. OGIS users' permissions to access the OAS will be limited by individual job requirements. OGIS management (Director and Deputy Director) will have access to a full view of the information in the system and will make case assignments. The system administrator will have access to all data in the OAS and will be able to make changes to system workflows. OGIS's internal procedures set forth the process for allowing access.

The system administrator will document each user's current requirements. Levels of access will seldom change and will most likely involve opening and closing accounts in the system. All requests for access or changes to access are documented by the system administrator in accordance with existing criteria and policies for access to data in OAS.

IV. 3 Will users have access to all data in the system or will the user's access be restricted.

Access will be based on the user type with varying levels of access granted.

IV. 4 What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by those who have been granted access?

OGIS case management procedures will be followed, which permits viewing of material in the system only when required for OGIS business processes. In addition, the system records (date/time stamps) every action performed in a case.

IV. 5 Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted into their contracts and other regulatory measures addressed.

Yes, contractors will perform system maintenance. All regulatory and legal requirements were included in the contract, including Privacy Act clauses.

IV. 6 Do other NARA systems provide, receive or share data in the system?

No.

IV. 7 Have the NARA systems described in item 6 received an approved Security Certification and Privacy Impact Assessment?

Not applicable.

IV. 8 Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

OGIS Director. Miriam Nisbet.

IV. 9 Will other agencies share data or have access to the data in this system?

No.

#### Section V: Opportunities for Individuals to Decline Providing Information

V. 1. What opportunities do individuals have to decline to provide information or to consent to particular uses of the information, and how can individuals grant consent?

In order for OGIS to assist customers, they must provide contact information, including name (first and last) and home or business address, and may provide a telephone number, and email address. This information is necessary in order for OGIS to provide assistance with a request or appeal because without it OGIS would have no way to contact the individual customer. In cases in which an individual declines to provide this information, OGIS will not be able to provide assistance. The Privacy Act of 1974 requires that OGIS customers provide a signed and dated customer authorization allowing OGIS to exchange information and records with other Federal agencies pertaining to the requester's FOIA and/or Privacy Act request/administrative appeal. Although OGIS provides sample consent language to its customers, a customer may chose to edit this language to adjust the authorization to his or her specifications Furthermore, the Administrative Dispute Resolution Act of 1996 allows for confidentiality during the course of mediation or other alternative dispute resolution technique. Therefore, a customer can request confidentiality when working with OGIS. In all cases, OGIS seeks all parties' approval before sharing any information between parties.

V. 2. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

As stated above, OGIS does not intend to consolidate or link data about system users with other systems. OGIS will compile the information provided by its customers in case files, which will also include information OGIS receives from other Federal agencies about the customer's FOIA/PA request or appeal. OGIS will create case files for the sole purpose of providing mediation services to resolve disputes between FOIA requesters and Federal agencies, including providing ombuds services. OGIS's mission is focused on improving the administration of FOIA, which is likely to enhance the public's use of FOIA (and the Privacy Act of 1974) to obtain access to information maintained by the executive branch. OGIS does not administer any negative determination that would affect a customer's due process rights.

## Section VI: Security of Collected Information

VI. 1 How will data be verified for accuracy, timeliness, and completeness? What steps or procedures are taken to ensure the data is current? Name the document that outlines these procedures.

OGIS considers data provided by a customer to be accurate, relevant, timely, and complete unless official government records prove that it is not. OGIS has established the following protocols for ensuring that data relating to users is timely, accurate, and complete.

When a case is entered into the OAS by an external user, an OGIS user must verify the information by reviewing the documents submitted by the customer with the initial request for assistance. Once a case is opened in the system, the OGIS user assigned to handle the case will review the information for accuracy, timeliness, and completeness. When an OGIS user identifies a problem with the information provided by a customer, this employee will contact the customer to resolve the problem. In addition, if OGIS learns that case information is not current, an employee will attempt to contact the customer to obtain current information. Upon the completion of a case, OGIS management will conduct a final review of the case information. OGIS's internal procedures and its Internal Control Plan (available upon request) outline this quality assurance process.

If a case is entered into the OAS by an OGIS user, the OGIS employee ultimately assigned to handle the case will review the information. Further, in assigning cases to OGIS users, OGIS management will conduct a review of the case information prior to case assignment.

The current name of the document that outlines this procedure is "Case Procedures for OGIS Staff".

VI. 2 If the system is operated in more than one site, how will consistent use of the system and data be maintained by all sites.

The system can be used where internet access is available. However, all users that work in the system will do so at their regular work station or at another approved workspace. OGIS's internal case procedures will be used to ensure consistent use of the system and maintenance of the data. All necessary equipment (i.e. scanners, printers) will be available at the alternative workspace.

VI. 3 What are the retention periods of data in this system?

10 years.

VI. 4 What are the procedures for disposition of the data at the end of the retention period?

Records created in connection with a request for OGIS assistance, i.e., internal and external correspondence, research, internal and external e-mail messages, internal memoranda and documents will be destroyed 10 years after the case has been closed. Ad hoc and standard reports

from the OAS will be destroyed when superseded by an updated report or when no longer needed for current business or when 2 years old, whichever is sooner.

The system administrator is alerted when a case reaches its disposition period and will go in and delete all files and records associated with the case 10 years after closure.

\*OGIS has submitted this record schedule for approval.

VI. 5 Is the system using technologies in ways that the Agency has not previously employed?

Yes, this is the first system that is using “private” cloud computing or an externally hosted program. In addition, this the technologies being used include scanning documents and attachments into an electronic format, automated workflow processes, web access to submit requests, and collaborative workspace for users participating in mediation.

VI. 6 How does the use of this technology affect public/employee privacy?

The technology enhances OGIS’s workflow processes and ensures the safeguarding of information entered into the system.

VI. 7 Does the system meet both NARA’s IT security requirements as well as the procedures required by federal law and policy?

Yes. All of NARA’s IT requirements and procedures have been followed and are in place.

VI. 8. Has a risk assessment been performed for this system? If so, and risks were identified, what controls or procedures were enacted to safeguard the information?

Yes, NARA performed a full certification of all applicable NIST and NARA security measures have been applied to the server environment.

VI. 9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.

NARA and the OAS contractor have performed all necessary monitoring, testing, evaluation, security demands and requirements in accordance with the requirements for a hosted environment.

VI. 10. Identify a point of contact for any additional questions from users regarding the security of the system.

Candace Boston, OGIS

301-837-3789, [Candace.boston@nara.gov](mailto:Candace.boston@nara.gov)

Keith Day, NHI

301-837-1877 [keith.day@nara.gov](mailto:keith.day@nara.gov)

## Section VII: System of Records Covered by the Privacy Act

VII. 1 Under which Privacy Act systems of records notice does the system operate?

NARA 40: The Office of Government Information Services (OGIS) Case Files.

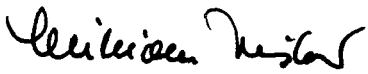
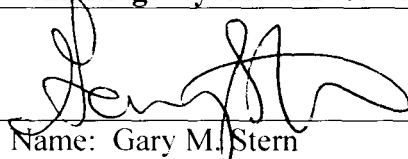

VII. 2. If the system is being modified will the Privacy Act System of Records notice require amendment or revision?

System is not being modified.

## Conclusions and Analysis

No pertinent issues arose while drafting this assessment.

**The Following Officials Have Approved this PIA**

<b>System Manager (Project Manager)</b>	
 (Signature)	Aug 19, 2011 (Date)
Name: Miriam Nisbet	
Title: OGIS Director	
Contact information: 301-837-3787	
<b>Senior Agency Official for Privacy (or designee)</b>	
 (Signature)	8/31/11 (Date)
Name: Gary M. Stern	
Title: SAOP and General Counsel	
Contact information: 301-837-3026	
<b>Chief Information Officer (or designee)</b>	
 (Signature)	8/26/11 (Date)
Name: Michael Wash	
Title: CIO	
Contact information: 301-837-1992	

## Appendix A

### NARA Privacy Act Systems: NARA 40

**System Name:** The Office of Government Information Services (OGIS) Case Files.

**System Location:** The OGIS case files are maintained in the National Archives and Records Administration, Office of Government Information Services, Room 2510, 8601 Adelphi Road, College Park, MD 20740.

**Categories of Individuals Covered by the System:** Individuals covered by this system include persons who request OGIS assistance in connection with the filing of a Freedom of Information (FOIA) and/or Privacy Act request or appeal to any Federal department or agency.

**Categories of Records in the System:** The OGIS case files include: correspondence, case notes, FOIA and Privacy Act request letters, appeal letters, agency replies to original requests and appeals, supporting documents, research, and other administrative forms used in the process. These files may also contain information or determinations furnished by, and correspondence with, other Federal agencies. OGIS case files may contain some or all of the following information about an individual, name, address, telephone number, e-mail address, Federal inmate register number, research interests, other information provided by the requester and by other agencies, and copies of documents furnished to the requester..

**Authority for Maintenance of the System:** 5 U.S.C. 552a(a)(3), as amended.

**Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of Such Uses:** OGIS maintains case files on individuals to record: requests for assistance, actions taken on cases; and, the status of cases in logs and databases. In addition, OGIS also serves as the FOIA Ombudsman in connection with its mission to review agency compliance with the FOIA. In this role, OGIS will capture and address systematic problems in FOIA administration as such individual case problems may serve as one of the bases to establish current systematic trends in the process. For this latter function, OGIS will remove personal information and use the remaining information collected for statistical purposes.

OGIS may disclose information in case files to agencies that have an equity in the subject FOIA and/or Privacy Act request and/or appeal in order for those agencies to participate in informal or formal mediation efforts. The routine use statements A, E, F, G and H, described in Appendix A following the NARA Notices, also apply to this system of records.

## **Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:**

**Storage:** Paper and electronic records.

**Retrievability:** Information in OGIS case files may be retrieved by one or more of the following data elements: the name of the individual and an alphanumeric case file number.

**Safeguards:** OGIS case files are at all times maintained in buildings with security guards or secured doors, and all entrances are monitored by electronic surveillance equipment. During business hours, paper records are accessible only by authorized NARA personnel. Electronic records are accessible via passwords from terminals located in attended offices. After business hours, or when OGIS personnel are not present in the offices, the OGIS offices are secured in addition to building security.

**Retention and Disposal:** OGIS case files are temporary records and are destroyed in accordance with the disposition instructions in the NARA records schedule contained in FIFRS 203, the NARA Files Maintenance and Records Disposition Manual. Individuals may request a copy of the disposition instructions from the NARA Privacy Act Officer.

**System Manager(s) and Address:** For OGIS case files, the system manager is the Director of the OGIS, Room 2510, 8601 Adelphi Road, College Park, MD 20740.

**Notification Procedure:** Individuals interested in inquiring about their records should notify the NARA Privacy Act Officer at the address listed in Appendix B.

**Record Access Procedures:** Individuals who wish to gain access to their records should submit their request in writing to the NARA Privacy Act Officer at the address listed in Appendix B.

**Contesting Record Procedures:** NARA rules for contesting the contents and appealing initial determinations are found in 36 CFR part 1202.

**Record Source Categories:** Information in OGIS case files is obtained from persons who request assistance in connection with the submission of a FOIA and/or Privacy Act request or appeal to a Federal agency, and from agencies that have acted on the request or appeal.