Privacy Impact Assessment for

Government-Wide Email System (GWES)

February 28, 2025

Contact Point
Riccardo Biasini
Senior Advisor to the Director
Office of the Director

Reviewing Official
Greg Hogan
Chief Information Officer

Legal Requirements for Privacy Impact Assessment

Longstanding Office of Management and Budget (OMB) and Office of Personnel Management (OPM) guidance explains that Privacy Impact Assessments (PIAs) are not required for IT systems or projects that collect, maintain, or disseminate information solely about federal government employees. For example, the OMB guidance states that "[n]o PIA is required . . . for government-run websites, IT systems or collections of information to the extent that they do not collect or maintain information in identifiable form about members of the general public." M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Attachment A(II)(B)(3) (Sept. 26, 2003); *see also id.* Attachment A(II)(B)(1) ("The E-Government Act requires agencies to conduct a PIA before: 1. developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or 2. initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government)."); OPM Privacy Impact Assessment (PIA) Guide, at 2 (Apr. 22, 2010) (stating that a PIA is required for "an IT system or project that collects, maintains, or disseminates information in identifiable form from or about members of the public"); *id.* at 3.

The Government-Wide Email System (GWES) collects, maintains, and disseminates information about federal government employees. Therefore, no PIA is required. OPM has nevertheless chosen to conduct this PIA in its discretion.

Abstract

OPM has a variety of personnel management functions, including executing, administering, and enforcing the civil service system. In order to carry out these duties, OPM internally developed the GWES to enable widespread,

rapid email communication with federal government employees. The GWES is designed to maintain the names and government email addresses of federal government employees, as well as emails sent from the system and responses to those emails.

Overview

To execute its authorized role with respect to personnel matters and fulfill its duty to enforce the civil service laws, OPM has developed a system to send government-wide emails to federal government employees and receive responses. This system increases efficiency and transparency by allowing fast and widespread communication with the federal workforce OPM has been tasked with overseeing.

The GWES system operates entirely on government computers and in Microsoft applications procured in the normal course. OPM uses this system to communicate with federal employees, in a capacity within its statutory authority. The GWES is designed to collect, maintain, and use the (1) names of federal employees, (2) their government email addresses, and (3) email messages and responses, which may include additional information about the employee provided by that employee. The GWES blocks responses from emails that do not have government domains.

The information in the GWES is accessible by a limited number of individuals within OPM who have a need for the information in the performance of their duties, overseen by the Chief Information Officer.

The GWES is built largely upon employee email contact information found in the Enterprise Human Resources Integration (EHRI) and Official Personnel Folder (OPF) record systems. Additional email contact data is collected from the employing agencies of federal workers. OPM applies filters to these various sources to remove erroneous domains before emails are sent. The GWES is subject to existing and approved OPM security plans and the data is

stored in secure Microsoft applications and on government computers requiring PIV access.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The President may delegate "authority for personnel management functions" to the Director of OPM. 5 U.S.C. § 1104(a)(1). OPM has been delegated authority to "exercise and provide leadership in personnel matters," among other functions. Executive Order 9830 § 01.2(b). The Director also has the duty to "execut[e], administer[], and enforce[e] … the civil service rules and regulations of the President and the Office and the laws governing the civil service." 5 U.S.C. § 1103(a)(5). Other relevant authorities include: 5 U.S.C. §§ 301, 2951, 3301, 4302, 6504, 8347, and 8461. These authorities permit OPM to maintain and request information regarding federal employees. The President may also, from time to time, direct OPM to collect information or communicate with the federal workforce on particular subject matters.

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Email systems are not generally subject to the Privacy Act of 1974. However, to the extent the GWES contain records subject to the Privacy Act, or information stored on secure government computers, the information in this system is covered by various OPM SORNs, including but not limited to OPM GOVT-1, GOVT-2, Central-21, and Internal-21 SORNs.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

The GWES is located within Microsoft applications and on secure government computers. These Microsoft Applications have been granted an Authorization to Operate (ATO) that includes an approved system security plan. The

government computers storing the data are subject to standard security requirements, including limited PIV access.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Depending on the nature and type of record within the GWES, various NARA-approved records schedules may apply. Item 040 (DAA-GRS-2017-0007-0004) covers any eOPF records and item 080 (DAA-GRS2017-0007-0012) covers other personnel contact information. Email records are governed by GRS 6.1, Capstone E-mail Retention.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Information contained in the GWES is not subject to the PRA because it is not collected from the public.

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

The GWES is designed to collect, maintain, and use the names and government email addresses of federal government employees. The GWES also maintains emails sent to those addresses, and collects and maintains responses to those emails. Specifically, the GWES contains the following:

- **Employee Contact Data:** The GWES is designed to collect, maintain, and use the names and government email addresses of federal government employees. Other identifying information is not used.

- **Employee Response Data:** After an email is sent using Employee Contact Data, the GWES stores that email and may collect and maintain responses. In some circumstances, responses may also be

sent directly to or redistributed to employing agencies or other agencies consistent with applicable restrictions on the particular data at issue and using authorized means of transmission.

2.2. What are the sources of the information and how is the information collected for the project?

The Employee Contact Data is compiled using the EHRI and OPF record systems. Additionally, some email contact data is collected from the employing agencies of federal workers. The system applies filters to remove erroneous domains before emails are sent.

The Employee Response Data is sent by federal government employees to OPM by email.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No, although many names and email addresses of federal government employees are publicly available.

2.4. Discuss how accuracy of the data is ensured.

The Employee Contact Data comes from the EHRI and OPF systems, which are subject to their own accuracy measures as outlined in their respective PIAs, as well as directly from the employing agencies.

The Employee Response Data comes directly from employees through their secure government email addresses. OPM anticipates that the responses will cover information within employees' personal knowledge or information provided to them in the course of their official duties.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that erroneous email addresses have been collected.

Mitigation: This risk has been mitigated by compiling the Employee Contact Data through the EHRI and OPF systems, and directly from the employing agencies. The GWES uses email addresses with government domains and uses a filtering mechanism to remove contact data erroneously captured before emails are sent.

Privacy Risk: There is a risk that the Employee Response Data will be erroneous.

Mitigation: Because OPM uses the GWES to send emails to employees' official government email addresses, OPM has a high degree of confidence that the Employee Response Data will represent actual employee responses. Additionally, employees have the ability to correct any erroneous responses by working with the human capital officer or manager in their employing agency.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

The GWES enables OPM to communicate directly and quickly with federal government employees and help OPM fulfill its statutory and delegated duties to lead and oversee personnel management functions in the federal workforce. OPM may also further communicate employee responses to employing agencies to facilitate those agencies' own personnel management, or other agencies as appropriate to facilitate government-wide workforce initiatives.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

OPM employees programmatically evaluate responses to verify the quality of the system and analyze the substance of the Employee Response Data. OPM

anticipates enhancing and refining its response analyses over time. OPM may also query specific responses or emails to evaluate them as needed. Responses may be used to assist in making personnel decisions and to inform broader workplace initiatives.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

No.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the GWES information may be accessed by unauthorized users or by authorized users for an unauthorized purpose.

Mitigation: This risk is mitigated by restricting disclosure to a limited number of individuals who have a need to know the GWES information. The data is stored in secure Microsoft applications, and on secure government computers requiring a PIV card to access.

Section 4.0. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The names and government email addresses of federal government employees are already housed in OPM systems or provided by employing agencies and, in any event, do not contain substantive information about employees. As a result, there is no reason to provide advance notice for the collection of Employee Contact Data. Employees are provided notice of collection of the Employee Response Data in the emails disseminated using the GWES. Employees provide the data themselves in response to the email. This PIA also serves as a public resource explaining the purpose of the GWES, applicable SORNs, and other privacy-related information.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individual federal government employees can decline to provide information by not responding to the email. The consequences for failure to provide the requested information will vary depending on the particular email at issue.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not know their information is being collected, maintained, and distributed through the GWES.

Mitigation: This risk is mitigated by the publication of this PIA and through various statements provided to government employees explaining the information collection at issue.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

The records in the GWES are maintained according to the retention schedules identified in Section 1.4.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the GWES information will be retained for longer than is necessary.

Mitigation: The risk is mitigated because OPM can delete all the GWES information, consistent with applicable retention schedules.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

OPM anticipates regularly sharing GWES information relating to particular employees with their employing agency. In certain situations, data may also be shared with other agencies. Any data sharing will be undertaken consistent with applicable laws and policies, including pursuant to routine uses of applicable SORNs or employee consent. Data will be shared via authorized systems hosted either by OPM or the receiving agency.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

To the extent that GWES information is shared outside of OPM, it is shared consistent with applicable provisions of the Privacy Act, including through the routine uses of pertinent SORNs. The principal personnel SORN, GOVT-1, is owned by OPM but information may be accessed by employing agencies as needed.

6.3. Does the project place limitations on re-dissemination?

Government agencies that receive GWES information are generally subject to both the government-wide SORNs referenced in Section 1.2 as well as their own SORNs. Their use or disclosure of the information may occur only as consistent with applicable legal limitations.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

OPM keeps a record of distributions to the employing agencies in Microsoft applications. All actions taken by a user in Microsoft systems are logged, monitored, and accessed by those with a need to know for the performance of their official duties.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that GWES information will be shared outside of OPM without authorization.

Mitigation: This risk is mitigated by limiting access to the GWES and disseminating GWES information only as consistent with relevant SORNs or as otherwise permitted by applicable law.

Section 7.0. Redress

7.1. What are the procedures that allow individuals to access their information?

The federal government employees in the GWES have access to their own individual information. Employees will have a copy of any email that is sent, as well as their response. In addition, access procedures are outlined in each relevant SORN referenced in 1.2.

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

If the Employee Response Data is erroneous, any federal government employee covered by the GWES may inform the human capital officer or a manager in their employing agency, who can work with the employee and OPM as necessary to correct the problem.

7.3. How does the project notify individuals about the procedures for correcting their information?

Emails sent through the GWES, or related guidance disseminated through agency human capital officers or managers, may inform individual federal employees of the procedures for correcting erroneous information through their employing agency. Also, employees may follow the publicly accessible access and amendment procedures outlined in the relevant SORNs referenced in 1.2.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that federal government employees will not have information regarding how to amend erroneous information.

Mitigation: Lodging the primary corrective mechanism in the human capital officer or manager at the employing agency gives each employee intuitive and easy access to the corrective mechanism. Also, each SORN has clear access and amendment procedures that employees may follow.

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

GWES information is captured by OPM's auditing tools and retained in an auditing archive. The Office of the Chief Information Security Officer reviews for suspicious or unusual activity and suspected violations, and appropriate action is taken as necessary.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

OPM employees are required to take IT Security and Privacy Awareness training on an annual basis, and agree to OPM's Rules of Behavior before accessing the system.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

Only a limited number of OPM employees with a need to know will have access to the full extent of the GWES data. No employee has access unless specifically authorized by the system owner and the authorizing official. Data sharing outside OPM is permitted only insofar as consistent with applicable law and as described above.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, and new access to the system by organizations within OPM and outside?

Any changes in GWES access, uses, sharing agreements, or Memoranda of Understanding (MOUs) would need to be reviewed and approved by the system owner in coordination with the Office of the Chief Information Officer, as consistent with applicable law.

Responsible Officials

Office of the Chief Information Officer

Office of the Director

Approval Signature

Signed copy on file with the Chief Information Officer

Greg Hogan
Chief Information Officer