Privacy Impact Assessment for

Government-Wide Email System (GWES)

February 5, 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 only the information of 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 and

simultaneous communication with federal government employees. The GWES maintains only the names and government email addresses of federal government employees, as well as voluntary responses to mass 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. This system increases efficiency and transparency by allowing simultaneous communication with the federal workforce OPM has been tasked with overseeing.

The GWES system operates entirely on government computers and in Microsoft mailboxes. OPM uses this system to communicate with federal employees, a capacity which is within its statutory authority. The only information collected, maintained, or used by the GWES are (1) names of federal employees, (2) their government email addresses, and (3) short, voluntary email responses.

The information in the GWES is accessible by a handful of individuals within OPM, overseen by the Chief Information Officer.

The GWES is built upon employee contact information found in the Enterprise Human Resources Integration (EHRI) and Official Personnel Folder (OPF) record systems. Additional contact data is collected from the employing agencies of federal workers, which is received through email. The GWES is subject to existing OPM security plans and the data is stored in secure mailboxes or 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[] … 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, 6504, 8347, and 8461. These authorities permit OPM to maintain and request information regarding federal employees.

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, but to the extent that records pertaining to individuals are retrieved for purposes of making decisions about individuals, the records relevant to this project are covered by the OPM GOVT-1 and OPM/Central-21 SORNs.

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

The Office 365 mailbox has been granted an Authorization to Operate (ATO) that includes a system security plan. The government computer storing the data is 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?

To the extent that email records in the system are used for personnel decisions, records in the system are governed by GRS 6.1 Capstone E-mail Retention. Item 040 (DAA-GRS-2017-0007-0004) covers any eOPF records and requires that they be destroyed when survivor or retirement claims are

adjudicated or when records are 129 years old, whichever is sooner, but longer retention is authorized if required for business use. Item 080 (DAA-GRS2017-0007-0012) covers other personnel contact information and requires destroying remaining documents 1 year after employee separation or transfer.

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 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.

GWES collects, maintains, and uses the names and government email addresses of federal government employees. GWES also collects and redistributes responses to emails sent to those addresses, which are limited to short, voluntary, non-identifying information. Specifically, GWES contains the following:

- **Employee Contact Data:** GWES collects, maintains, and uses 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, GWES collects, maintains, and redistributes short, voluntary responses.

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 data is collected from the employing agencies of federal workers, which is received through email.

The Employee Response Data is sent 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.

Many of the names and email addresses of federal government employees are publicly available.

2.4. Discuss how accuracy of the data is ensured.

OPM has a high degree of confidence in the accuracy of the Employee Contact Data because it 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.

OPM has a high degree of confidence in the accuracy of the Employee Response Data because OPM receives the information directly from employees through their secure government email addresses.

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 only through the EHRI and OPF systems, and directly from the employing agencies. GWES only uses email addresses with government domains.

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

Mitigation: Because OPM uses GWES to send emails only to employees' official government email addresses, OPM has a high degree of confidence that the Employee Response Data will represent actual employee responses. Additionally, GWES has implemented procedures for employees to correct any erroneous responses by working with the human capital officer in their employing agency. If an erroneous response is sent, it can easily be corrected in GWES when the human capital officer notifies OPM. GWES blocks all responses from emails that do not have government domains.

Section 3.0. Uses of the Information

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

GWES enables OPM to communicate directly with federal government employees simultaneously and help OPM fulfill its statutory and delegated duties to lead and oversee personnel management functions in the federal workforce. OPM further communicates employee responses to employing agencies to facilitate those agencies' own personnel management.

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.

GWES programmatically evaluates responses to verify the quality of the system and the substance of the Employee Response Data.

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 access to a limited number of individuals assigned to access the GWES information and blocking others from access. The data is stored only in secure Microsoft mailboxes, 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. All individuals are provided advance notice of the Employee Response Data, as it is voluntarily provided by the individuals themselves in response to an email.

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

The Employee Response Data is explicitly voluntary. The individual federal government employees can opt out simply by not responding to the email.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not realize their response is voluntary.

Mitigation: This risk is mitigated by ensuring that any email sent using GWES is clear, by explicitly stating that the response is voluntary, and by including specific instructions for a response.

Section 5.0. Data Retention by the Project

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

The Employee Contact Data will be retained indefinitely so that OPM can use GWES to contact federal government employees. The Employee Response Data will be retained consistent with GRS 6.1 Capstone E-mail Retention, which establishes retention at 7 years for most users and 15 years, followed by permanent retention with NARA, for Capstone officials.

5.2. Privacy Impact Analysis: Related to Retention

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

Mitigation: The risk is mitigated because OPM can delete all 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.

The GWES information of any particular individual may be shared outside of OPM with that employee's employing agency, consistent with applicable laws and policies. Emails sent using GWES inform the employee that he consents to OPM's sharing of his response in this way by replying to the email.

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 consistently with applicable provisions of the Privacy Act, including through employee consent.

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

Government agencies that receive GWES information are generally subject to the government-wide SORN referenced in Section 1.2 and their use or disclosure of the information may occur only as consistent with the Privacy Act, applicable SORNs, and any inter-agency agreements.

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

The GWES keeps a record of all email distributions to the employing agencies in mailbox. All actions taken by a user in the mailbox system are logged, monitored, and accessed by those with a need to know.

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 disseminating GWES information only as consistent with relevant SORNs or as otherwise permitted by the Privacy Act, and by requiring receiving agencies to adhere to relevant legal requirements and inter-agency agreements.

Section 7.0. Redress

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

The federal government employees in GWES have access to their own individual information.

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 in GWES is directed to inform the human capital officer in their employing agency. The employing agency will correct the inaccurate or

erroneous information. The erroneous information can also be corrected in GWES when the human capital officer notifies OPM.

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

Any email sent through GWES, or related guidance disseminated through agency human capital officers, will inform individual federal employees of the procedures for correcting erroneous information through their employing agency.

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 corrective mechanism in the human capital officer at the employing agency gives each employee intuitive and easy access to the corrective mechanism.

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 the tools 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.

All OPM employees are required to take IT Security and Privacy Awareness training on an annual basis, and sign OPM's Rules of Behavior.

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 employees with a need to know will have access to the full extent of GWES data. As necessary, and with consent of the individual federal employee, GWES information will be shared with those who need to know at that individual's employing agency.

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 all appropriate OPM stakeholders 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