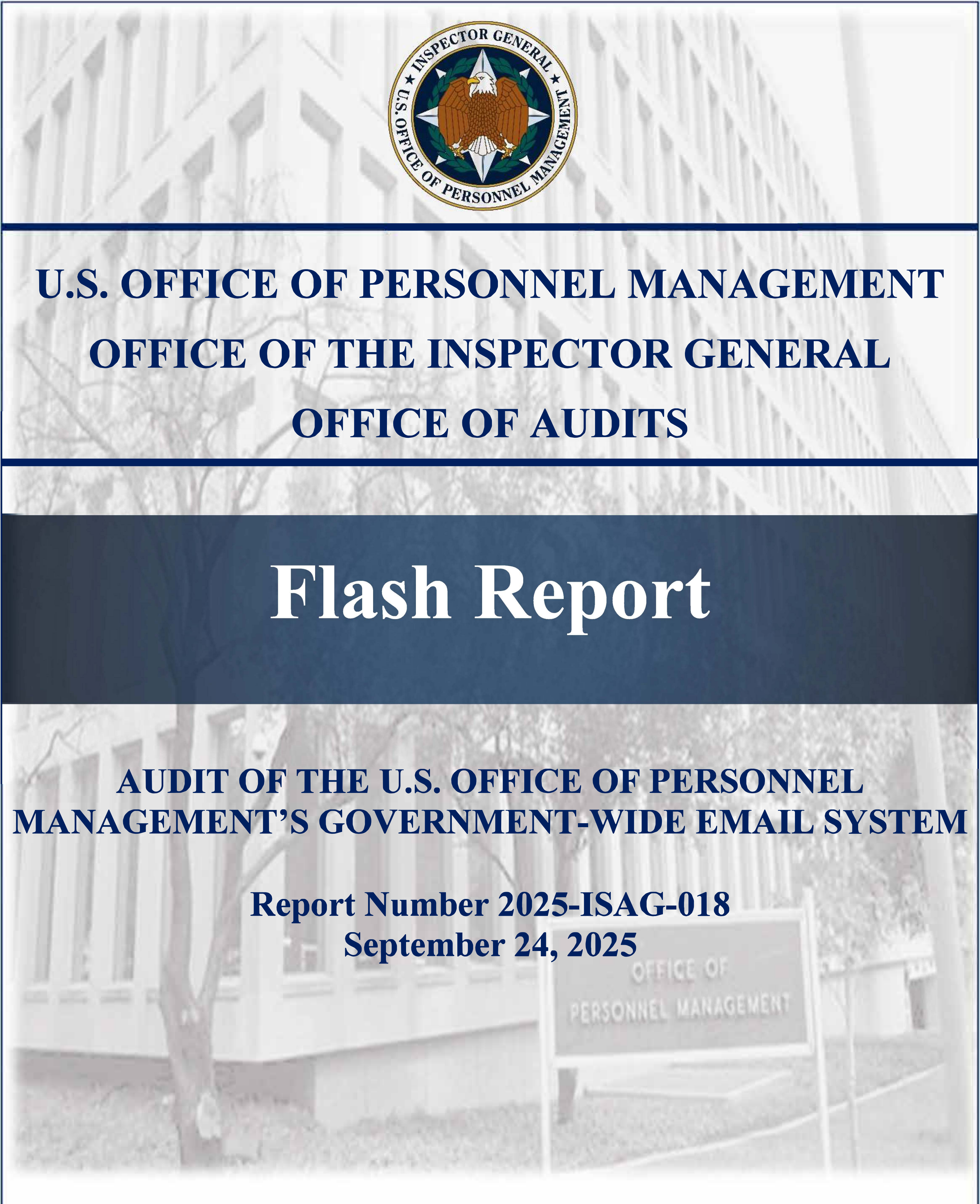


U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Flash Report

AUDIT OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S GOVERNMENT-WIDE EMAIL SYSTEM

Report Number 2025-ISAG-018
September 24, 2025

EXECUTIVE SUMMARY

Audit of the U.S. Office of Personnel Management's Government-Wide Email System

Report No. 2025-ISAG-018 **September 24, 2025**

Why Are We Issuing This Report?

The primary objective of this report is to communicate our concerns regarding the U.S. Office of Personnel Management (OPM) Office of the Chief Information Officer's (OCIO) rollout of the Government-Wide Email System (GWES). The other objective of this audit is to determine how the GWES was developed and implemented, determine its impact on OPM's cybersecurity posture, and address congressional inquiries in accordance with applicable laws and regulations such as the Federal Information Security Modernization Act of 2014 (Public Law 113-283). While the audit is not complete, we have become aware of issues that should be addressed promptly. This report does not represent the final conclusions of the audit. Our work will continue, and a final report, which may include further findings, will be issued at the conclusion of the audit.

What Did We Review?

In accordance with the Inspector General Act of 1978, as amended, 5 U.S.C. § 404(a) and the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Federal Offices of Inspector General (Silver Book), the OPM Office of the Inspector General completed this flash report to inform stakeholders regarding OPM's failure to follow information systems security best practices for the development, implementation, and maintenance of the GWES. We conducted this portion of the audit from April 8, 2025, through July 28, 2025.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

We found issues in the OCIO's rollout of the GWES, including the reintroduction of significant information security risks into OPM's control environment. Specifically, our audit has identified the following:

OPM senior management overrode established information technology security and privacy controls.

During fieldwork, we found various forms of evidence that demonstrate that the OCIO bypassed its Enterprise Change Management process, inaccurately classified the GWES, and circumvented its own policies and procedures that implement the National Institute of Standards and Technology Risk Management Framework. The totality of the information reviewed leads to the finding that OPM overrode these controls so that it could quickly send emails to the federal workforce.

OPM failed to establish protocols for handling sensitive data received through the GWES.

During our fieldwork we learned through various forms of evidence, including responses provided through information requests, that the OCIO had not developed or implemented procedures to manage and secure HR@OPM.GOV email replies that may have contained sensitive or potentially classified data individually or when aggregated. Therefore, OPM was unable to determine whether sensitive or classified information had been transmitted, stored, and/or processed by the GWES. Additionally, it was unclear whether everyone who had access to the emails was properly cleared to review potentially classified information submitted through HR@OPM.GOV responses.

ABBREVIATIONS

ATO	Authorization to Operate
ECM	Enterprise Change Management
EHRIDW	Enterprise Human Resources Integration Data Warehouse
FISMA	Federal Information Security Modernization Act of 2014
GWES	Government-Wide Email System
ISAG	Information Systems Audits Group
IT	Information Technology
NIST SP	National Institute of Standards and Technology Special Publication
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OPM	The U.S. Office of Personnel Management
RMF	Risk Management Framework
SME	Subject Matter Expert
SORN	System of Records Notice

TABLE OF CONTENTS

I. BACKGROUND

The U.S. Office of Personnel Management (OPM) Office of the Inspector General (OIG) is responsible for the prompt communication of significant findings, ensuring that agency officials, congressional stakeholders, and the public are alerted to potential risks and management concerns without delay. Consistent with that duty, we are issuing this flash report detailing issues identified in OPM's implementation and potential decommissioning of the Government-Wide Email System (GWES). We relied upon the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Federal Offices of Inspector General (Silver Book) when conducting our work and preparing this flash report. We adhered to the professional standards of independence, due professional care, and quality assurance and followed procedures to ensure accuracy of the information presented. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

On January 20, 2025, OPM began a senior leadership transition that included a new Acting Director, General Counsel, and Chief Information Officer (CIO). On January 24, 2025, shortly after the new leadership was in place, a new capability to email the entire federal workforce via HR@OPM.GOV was operational. [1] We subsequently learned this capability was a function of the newly implemented GWES. The standup and deployment of the GWES occurred in four days, which is more quickly than it has historically taken to have a new system or major modification to an existing system developed, tested, and authorized to operate in OPM's network.

The findings in this report are specific to OPM's circumvention of its established information systems security and privacy policies, procedures, and controls to expedite the implementation of the GWES. The findings and conclusions also address the need for adherence to appropriate laws, regulations, policies, and procedures related to the decommissioning of the GWES. OPM knows firsthand the importance of information technology (IT) security and privacy controls as it was subject to a major data breach in 2015 due to its lack of adequate controls for weaknesses that the OIG had been reporting on for many years prior. [2] Since 2015, the Office of the Chief Information Officer (OCIO) made significant progress in improving its cybersecurity posture by implementing many IT security and privacy controls recommended by the OIG. [3] However, during this ongoing audit we have identified serious issues with OPM's implementation of the GWES that have reintroduced information security weaknesses similar to those that existed a decade ago. [4]

This report was issued as a draft flash report due to the significant issues identified and the urgency of addressing them. However, in response to our communication of the issues to agency management, OPM stated its intention to decommission the GWES. Therefore, the intent of this flash report is to ensure OPM leadership uses report findings to prevent future management override of controls, updates its Enterprise Change Management (ECM) and audit engagement processes, and properly decommissions the GWES.

[1] See Appendix for a detailed timeline on the implementation of the GWES.

[2] The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation (2016), https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

[3] Semiannual Report to Congress: "The OPM OIG continues to make progress in working with OPM to close open recommendations from the OIG." https://www.oversight.gov/sites/default/files/documents/reports/2023-11/SAR69.pdf.

[4] Federal Information Security Modernization Act Audit FY 2015, https://www.oversight.gov/sites/default/files/documents/reports/2017-09/federal-information-security-modernization-act-audit-fy-2015-final-audit-report-4a-ci-00-15-011.pdf.

II. IDENTIFIED ISSUES AND RECOMMENDATIONS

A. MANAGEMENT OVERRODE CONTROLS

While conducting our audit of OPM's implementation of the GWES, we have concluded that OPM senior management circumvented established IT security and privacy controls to quickly launch the ability to send emails to the federal workforce. Specifically, OPM bypassed its ECM process, inaccurately classified the GWES as a subsystem of the Enterprise Human Resources Integration Data Warehouse (EHRIDW) and bypassed the National Institute of Standards and Technology Risk Management Framework (RMF) process, as well as its own policies and procedures for securely developing and authorizing new and existing systems.

1. OPM Bypassed the ECM Process

OPM's *Enterprise Configuration Management Policy and Procedures* states that "All changes to the OPM IT infrastructure, networks, systems, and applications are required to follow and are subject to the authority of the [ECM] process." However, the OCIO bypassed system change controls by implementing the GWES outside of its established ECM process. The purpose of the ECM process is to provide transparency to changes, improve coordination of change implementation, and provide effective IT decision-making. OPM's *Enterprise Configuration Management Policy and Procedures* state that successful implementation of the ECM process results in changes that are recorded and assessed. All change proposals must be submitted to the ECM website by the IT Program Manager using the required documentation applicable to the category of the change being implemented. Further, change proposals are to be reviewed and approved before changes are developed and deployed. Approved changes should also be tested and validated post implementation. The OCIO bypassed the ECM process because the project "had a very short timeframe to deliver" and was approved only by the CIO and the Acting Director, resulting in the GWES changes not being recorded or tested. Moreover, OPM's Change Review Board and Engineering Review Board did not evaluate the implementation of the GWES and consequently were unable to provide recommendations for security, compliance, technical specifications, and impact on OPM's security posture. And while the OCIO has an emergency proposal process, it is reserved for repairing an error to an IT service, not establishing an IT system.

Failure to follow OPM's established ECM process increases the risk that security and privacy controls were not adequately implemented, allowing unknown vulnerabilities onto OPM's network.

Recommendation 1

We recommend that OPM retroactively follow its established ECM process and submit the GWES to the Change Review Board and Engineering Review Board to conduct a security, compliance, and technical specifications analysis to ascertain the impact on OPM's network and remediate any control weaknesses that are found.

<u>OPM's Response:</u>

"Non-Concur. The purpose of the ECM process is to ensure that any proposed changes are elevated at a sufficiently high level within CIO. The Change Review Board and Engineering Review Board may only make non-binding recommendations to the OPM CIO. In all cases, however, the CIO remains the ultimate decision-maker.

In this instance, the CIO directly approved the change to add the GWES system after careful consideration of the impact on OPM's network. He did so in consultation with OPM's Acting Director, who had personal experience building the Enterprise Human Resources Integration (EHRI) system as a supervisor at OPM. Both the CIO and the Acting Director concurred that an ECM process was not required. GWES was an outgrowth of EHRI that merely provided a mechanism to email many government employees at once using the OPM Azure Communication Service (ACS).

While the ECM process can serve a valuable function, it is not required in all instances. Technological systems must be agile and responsive to rapidly-evolving government needs—not captive to inflexible bureaucratic processes. In the first part of 2025, there was an urgent need to rapidly communicate with government employees regarding important workforce initiatives like the Trump Administration's Deferred Resignation Offer, 5 Bullets, and other workforce optimization initiatives. Using existing systems and technologies whose purpose is to facilitate efficient human capital management to perform what would be considered an entirely routine task (emailing all employees at once) at most any other enterprise in response to an urgent need did not require a complicated change management process.

In any event, prior to receipt of this draft report, OPM's Director determined that the need for the '5 Bullets' program had ended and notified all OPM employees as well as other federal agencies of this determination last week. As a result, OPM has decommissioned the GWES; therefore, OPM cannot concur."

<u>OIG Comment:</u>

We appreciated the opportunity to meet with the Director, Office of General Counsel (OGC), and OCIO representatives on August 4, 2025, to discuss our concerns identified in the draft flash report. On August 5, 2025, OPM's Director issued a statement to the press to inform the public that OPM decided to end the "five things" email reporting process.[5] Also, the Director confirmed that OPM ended the "five things" email reporting process in a blog post on

[5] Reuters article dated August 5, 2025: https://www.reuters.com/legal/litigation/trump-administration-formally-axes-elon-musks-five-things-email-2025-08-05/

August 8, 2025.[6]

Further, the Chief Information Officer (CIO) sent a memo to the Director on August 8, 2025, to notify the Director of his decision to officially decommission the system. Therefore, due to OPM decommissioning the GWES, this recommendation is closed.

However justified, the CIO and Acting Director bypassed OPM's current ECM process and related controls to fulfill the urgent need to rapidly communicate with all government employees. There is not an ECM process in place at OPM to accommodate the development and deployment of new systems in an urgent manner. Bypassing the ECM process eliminated the steps in the development of the GWES that would identify potentially critical controls needed to protect the OPM information systems environment. If rapid system development and deployment are a management priority, OPM should update its ECM process to include an agile methodology, while ensuring compliance with OMB and NIST requirements, as appropriate.

In addition*, The Standards for Internal Control in the Federal Government* maintain that the ability of management to override controls provides an opportunity to commit fraud.[7] Fraud risk factors do not necessarily indicate fraud exists but are often present when fraud occurs. Therefore, it is critical that OPM reduce the risk of fraud being committed by not overriding controls.

As stated in the CIO's memorandum, *Decommissioning the Governmentwide Email System,* "Going forward, OPM will continue to explore ways to allow Executive Branch leadership to communicate with all federal employees … ." We appreciate OPM's need to carry out its directives and mission and encourage OPM leadership to ensure that any future urgent system development projects follow an established process that identifies necessary internal controls and results in the deployment of robust and secure systems.

2. <u>OPM Inaccurately Classified the GWES</u>

The *OPM Security Authorization Guide* defines a subsystem as "a major subdivision of a major information system consisting of information, information technology, and personnel that perform one or more specific functions." OPM inaccurately classified the GWES as a subsystem of EHRIDW. In response to an information request, OPM stated that the GWES is a subsystem of EHRIDW because "sending emails to the people contained in the system is a natural extension of the system." However, OPM's *System Security Privacy Plan* describes the purpose of EHRIDW as a common repository for governmentwide personnel data,

[6] Support Agencies Through Change: https://www.opm.gov/news/secrets-of-opm/supporting-agencies-through-change/

[7] GAO Standards for Internal Control in the Federal Government (see Fraud Risk Factors section 8.04): https://www.gao.gov/assets/gao-14-704g.pdf

whereas the purpose of the GWES according to its *Security Impact Analysis* is to "send email notifications and gather responses … ."

The GWES leverages several separate OPM systems and applications including Microsoft Office 365, Azure Communication Services, and the GWES subject matter expert's (SME) workstation. The SME's workstation contains Microsoft Visual Studio Code that is used to run programming scripts that send emails from HR@OPM.GOV and analyze responses from those emails.

On April 22, 2025, during the first of two GWES demonstrations, the GWES SME stated that the GWES operates as a standalone system and that the GWES does not maintain a permanent physical or logical connection for ongoing data exchange with EHRIDW. Rather, a comma-separated value file containing names and email addresses was exported from EHRIDW and shared with the GWES SME via an email attachment that was then added to a Python programming script. Furthermore, the OCIO provided evidence to support the GWES SME's description of the system; this included documentation depicting the official GWES boundary and dataflow diagrams, which show no EHRIDW system components connected to the GWES.

Additionally, the GWES was determined to be a subsystem of EHRIDW without consideration of the system registration process. The system registration process requires considerations for leveraging authorized environments for hosting applications, potential security impact level conflicts, the reuse of security controls, and relationships with other OPM systems. The OCIO cybersecurity branch chiefs review newly proposed systems for security considerations within the existing technical architecture. The system registration form captures system stakeholders and identifies assets that are components of the planned system. The process is designed to identify components of the planned system that require protection as early as possible. The system registration form that was provided to us was completed over three months after the GWES was in production. Completing the system registration process after the GWES was in production demonstrates that OPM had predetermined that GWES would be a subsystem of EHRIDW, bypassing the system registration process.

Failure to accurately classify the GWES increases the risk that proper security and privacy controls to protect confidentiality, integrity, and availability of federal data were not implemented.

Recommendation 2

We recommend that OPM accurately classify the GWES in accordance with the *OPM Security Authorization Guide*.

OPM's Response:

"Non-Concur. GWES was correctly determined to be an outgrowth of the EHRI system which could be covered under the same ATO. EHRI is a database that is designed to be used by OPM for governmentwide workforce management and planning. Its name gives away its purpose- Enterprise Human Resources Integration. EHRI integrates data from agency payroll systems and makes it usable for OPM to drive efficient and effective workforce planning. EHRI is the authoritative data store of email addresses, and GWES used that store to establish as an official government-wide communication channel to allow the Executive Branch to communicate rapidly and efficiently with its employees regarding important workforce initiatives. Thus, both systems fall within the same mission/business process under NIST 800-39 Tier 2. OMB A-130 specifies agencies have significant flexibility in determining what constitutes an information system and its associated boundary. Across government, it is a common practice to combine multiple related applications into a single ATO.

Finally, prior to receipt of this draft report, OPM's Director determined that the need for the '5 Bullets' program had ended and notified all OPM employees as well as other federal agencies of this determination last week. As a result, OPM has decommissioned the GWES; therefore, OPM cannot concur."

OIG Comment:

We disagree that the GWES was correctly determined to be an outgrowth of the EHRI system for the numerous reasons listed in this report. However, due to OPM decommissioning the GWES, there is no longer a need to reclassify the system. This recommendation is closed.

3. Impact of Inaccurate System Classification

OPM asserts that the GWES is approved to operate in OPM's environment under EHRIDW's authorization to operate (ATO) and inherits numerous IT security and privacy controls. However, as described above, we determined that the GWES is not a subsystem of EHRIDW and cannot inherit these controls. By misclassifying the GWES, OPM has circumvented its established authorization process and implemented a system without the IT security and privacy controls that it claims were inherited.

Shortly after the GWES implementation, a security impact analysis was conducted by OPM's technical stakeholders with the assumption that the GWES was a subsystem of EHRIDW. The analysis resulted in a recommendation that the GWES stakeholders implement and test "security and privacy controls and conduct a comprehensive security control assessment to test and validate implementation and effectiveness of security safeguards, as soon as possible," as required by National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations.* As of August 4, the date of our draft flash report, the OCIO had not properly selected, implemented, or tested IT security and privacy controls specific to the GWES.

NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations*, states that "the RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring." To ensure compliance with the RMF, OPM created the *OPM Security Authorization Guide*, which provides a standardized process for making informed risk-based decisions regarding authorizations.

The condition described above demonstrates how the OCIO has circumvented security and privacy controls by not following its own security authorization process, or the disciplined and structured approach required by the RMF.

The circumvention of established controls weakens OPM's cybersecurity posture and increases the risk that OPM could once again be subject to a significant cyberattack or data breach.

Recommendation 3

We recommend that OPM initiate an ATO for the GWES as a result of the reclassification outlined in recommendation 2. The ATO should include security categorization, control selection, implementation, and assessment.

Note – if the reclassification of GWES determines that it is a subsystem of another OPM system, a reauthorization of the selected parent system should be conducted.

OPM's Response:

"Non-Concur. As stated in OPM's response to Recommendation 2, there was no need for a separate ATO for the GWES system. Therefore, OPM cannot concur."

OIG Comment:

As stated in our response to Recommendation 2, we disagree that GWES was correctly determined to be an outgrowth of the EHRI system for numerous reasons listed in this report. However, due to OPM decommissioning the GWES, there is no longer a need to re-authorize the GWES system. This recommendation is closed.

> However, considering OPM has made substantial changes to EHRI's system documentation and continues to assert that the GWES was a subsystem of EHRI, OPM should update EHRI's ATO and make appropriate changes to reflect that the GWES is no longer a subsystem of EHRI.

B. PROTOCOLS FOR HANDLING SENSITIVE DATA

On February 22, 2025, the entire federal workforce received the "What did you do last week?" email from HR@OPM.GOV. This email was sent to the workforce from OPM via the GWES requesting five bullets from each employee describing what they had accomplished the previous week and was an ongoing, weekly request through August 5. Although the emails asked federal employees not to send classified information, OPM has no policies, procedures, or controls in place to know for certain whether classified or other sensitive information was being shared. It is a possibility that federal employees working with classified and/or sensitive information as part of their job duties shared such information in their responses to OPM in an attempt to justify their ongoing employment with the federal government.[8] Additionally, if these emails were accessed by unauthorized individuals, the aggregation of responses over time could provide an adversary insight into classified or sensitive activities.

Furthermore, OPM claims the GWES is covered under System of Records Notice (SORN) GOVT-1, General Personnel Records, which covers EHRIDW. That SORN states that EHRIDW is not a classified system. Therefore, the GWES is not authorized to process, store, or transmit classified data.

Compounding this issue is that email responses, potentially containing sensitive or classified information, may have been stored in multiple locations, including Microsoft Office 365 mailboxes, the GWES SME's laptop, and archived email storage. Additionally, these email responses were shared with multiple OPM officials via Microsoft OneDrive. The security clearance level (e.g., confidential, secret, and top secret) of these individuals with access to this information is unknown.

According to OPM's website:

> "Pursuant to the Privacy Act, Federal agencies must publish a system of records notice (SORN) about each system of records in the Federal Register. The SORN contains key information about the system of records including the authorities that allow the system to exist, the types of records in the system, the individuals whose records are in the system, how

[8] See Elon Musk's X post at https://nypost.com/2025/02/24/us-news/elon-musk-says-government-workers-who-dont-respond-to-a-second-what-you-accomplished-email-will-face-termination/.

> the records may be used within the agency, and when the records may be disclosed outside the agency."[9]

Additionally, NIST SP 800-53, Revision 5, control PS-3, enhancement 1, states that organizations must: "Verify that individuals accessing a system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of information to which they have access on the system."

Failure to implement controls surrounding the handling of sensitive and/or classified information increases the risk that individuals without adequate clearance could use this information for malicious purposes. Additionally, without adequate controls in place for identifying the type of information contained in the GWES, OPM may have been receiving and storing classified information without knowing it, and they may not be in compliance with statutory requirements applicable to the SORN.

Recommendation 4

We recommend that OPM immediately take appropriate steps to determine whether sensitive and/or classified information is stored by the GWES or disseminated to other agencies. Furthermore, if any sensitive and/or classified information is stored or has been disseminated by the GWES take immediate steps to ensure data security and privacy.

OPM's Response:

"Non-Concur. OPM recognizes the importance of ensuring data security and privacy. Therefore, OPM sent clear instructions not to send any classified information, links, attachments, or any sensitive PII. GWES has been decommissioned and there is no continuing need to maintain the records in that system. In his memo to the OPM Director, the CIO has already taken appropriate steps. Therefore, this recommendation should be closed."

OIG Comment:

Although OPM instructed federal employees not to send any classified information, links, attachments, the initial "five bullets" email, sent February 22, 2025, and OPM guidance, did not reference sensitive materials or PII. This initial email also gave employees one business day to respond. In a rush to achieve compliance with this new directive, many employees may have provided non-classified but sensitive information, especially as many may have believed failure to provide an immediate response would lead to termination. In subsequent email requests titled "What did you do last week? Part II," OPM instructed federal employees not to send any

[9] See OPM's System of Records Notices at https://www.opm.gov/information-management/privacy-policy/#url=SORNs.

"classified/sensitive" information. However, OPM never developed controls to manage sensitive and/or classified information that the GWES may have received, stored, or disseminated.

The "five bullets" emails also did not provide a standard definition of sensitive information; therefore, employees may have applied differing standards in determining what types of information to include in their responses. Standardized definitions of "sensitive information" are necessarily broad, and given the diverse array of agency missions, different agencies may have issued different guidance regarding the term "sensitive information." [10] Accordingly, responding employees may have misunderstood exactly what information should be considered sensitive. As the United States Government Accountability Office has noted, information management is frequently a challenge for federal agencies, who are often "limited in their ability to protect private and sensitive data entrusted to them."[11]

While information management requirements vary depending on the scope and type of information an agency maintains, having a full understanding of the type of information held in a system is a fundamental prerequisite to appropriately managing and safeguarding that information.[12] Obtaining a clear picture of a system's information is particularly important for systems like the GWES, which contain vast amounts of data potentially useful to adversaries.

The CIO's memorandum, *Decommissioning the Governmentwide Email System*, refers to "close-out procedures" and following "all applicable OCIO protocols for decommissioning the GWES." Although we are aware of a documented procedure and template for decommissioning systems, the documents have not been updated in years, and we are unsure if the documents are the same close-out procedures and OCIO protocols that the CIO referenced in his memo. Therefore, we also encourage the CIO to follow an updated formal process for decommissioning the system in accordance with current federal laws, regulations, and guidance. As part of the continued audit process, we will also review and evaluate OCIO's close-out procedures and protocols for the GWES.

Recommendation 5

We recommend that OPM develop and implement policies, procedures, and controls for handling potentially sensitive and/or classified information received by the GWES.

[10] See e.g., NIST SP 800-150, defining "sensitive information" as "information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy."

[11] U.S. Government Accountability Office, High Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation, 5 (2024).

[12] See e.g., NIST SP 800-37, Task P-12 (Requiring agencies to, as part of the NIST Risk Management Framework, "identify the types of information to be processed, stored, and transmitted [in order to] develop security and privacy plans for the system").

OPM's Response:

"Non-Concur. Please refer to OPM's response to Recommendation 4. This recommendation has been superseded by the decommissioning of the GWES system."

OIG Comment:

Considering that the GWES is being decommissioned, this recommendation is closed.

C. ENGAGEMENT CONSTRAINTS

From the start of our initial attempt to examine the GWES, we have experienced varied obstacles in coordinating meetings, gaining access to personnel and documentation, and have not received timely responses to formal written information requests. These persistent constraints make it difficult for us to conduct this audit in a timely manner.

As a result of numerous submissions to the OIG Hotline and a congressional inquiry, on March 3, 2025, we initiated a risk assessment of OPM's implementation of the GWES to ascertain if the system would affect OPM's compliance with applicable laws and regulations such as the Federal Information Security Modernization Act of 2014 (FISMA)[13] and to determine whether the allocation of resources to conduct an audit was necessary. The risk assessment was also intended to determine whether current OIG statutorily required work such as the annual FISMA and financial statement audits required modification to account for the new system.

Our attempt to conduct a risk assessment was questioned by OPM management, resulting in a series of email exchanges and senior executive level meetings, multiple rescheduling of a system demonstration, and ultimately a formal request from OPM that we conduct an audit instead of a risk assessment. To minimize further delays and in recognition of our past practice of considering requests from the Office of the Director or other OPM program offices for audits of particular programs or issues, and with the understanding that a system demonstration would be immediately rescheduled, we issued the OCIO an audit notification letter on April 3, 2025. However, these activities resulted in pushing meaningful fieldwork out for a month and a 41-day delay in scheduling the system demonstration.

During the first GWES demonstration, an OPM official interjected multiple times and prevented the subject matter expert from answering questions related to the audit. The frequent interjections cost valuable time and left considerable information gaps. This forced us to conduct a second demonstration which was also interrupted by another OPM official.

[13] 44 U.S.C. § 3551 et seq.

These constraints were further compounded by changes to OPM's audit coordination processes because of the reduction in experienced staff, which has led to untimely responses to all our information requests. To date, we have issued OPM eight information requests to obtain evidence related to our audit objectives. We assign due dates for each information request based on the size and complexity of the information requested. OPM failed to provide any responses to our requests by the due dates. Furthermore, OPM failed to provide complete responses to six out of our eight requests. Per OPM's request, we reached out to their Office of the General Counsel on numerous occasions to assist in facilitating the timely receipt of information. But, despite the General Counsel's and the Acting Director's efforts, significant delays persist. We recognize that assuming coordination of an ongoing audit can present initial challenges and may lead to some delays, which are not uncommon during the audit process. We regularly work closely with auditees to address any of their concerns and may modify due dates to ensure our work continues on schedule. However, the consistent untimeliness of every response in this audit has become a significant concern. The number of agency offices involved in this audit has resulted in ambiguity regarding roles, responsibilities, and accountability.

The Government Accountability Office's Government Auditing Standards, Section 1.03, states that "as reflected in applicable laws, regulations, agreements, and standards, management and officials of government programs are responsible for providing reliable, useful, and timely information for transparency and accountability of these programs and their operations."

Additionally, The Government Accountability Office's Government Auditing Standards, Section 9.12, states that "Auditors should also report any significant constraints imposed on the audit approach by information limitations or scope impairments, including denials of, or excessive delays in, access to certain records or individuals."

Failure to provide the OIG with timely access to personnel and information prolongs audit activities and delays the identification, reporting, and remediating of issues, thereby increasing exposure to preventable risk and delaying remediation. It is our hope that with the new Senate confirmed OPM Director in place, the timeliness of audit activities will significantly improve.

Recommendation 6

We recommend that OPM address the deficiencies in its audit engagement process and procedures to ensure consistent and efficient access to personnel and information in support of OIG audits.

OPM's Response:

"Concur in principle. OPM appreciates the concern OIG expresses for this issue and the importance of an effective and efficient audit engagement process. OPM recently changed the delegation for incoming audits in order to centralize the intake of these matters and inform the

appropriate parties. OPM acknowledges that there were some unique delays because of the change from a Risk Assessment to an Audit, and as a result of instituting response protocols with new personnel. OPM will consider take(sic) additional appropriate steps to ensure that OPM processes and procedures provide timely support to OIG audits."

<u>OIG Comment:</u>

No evidence was provided that would confirm that the changes address the finding and recommendation. Therefore, we cannot comment on the effectiveness of the new process referred to in OPM's response. As part of the audit resolution process, OPM's OCIO should provide OPM's Internal Oversight and Compliance office with evidence that this recommendation has been implemented.

APPENDIX I

The table below provides important dates and emails illustrating the GWES without an appropriate Authorization to Operate.

Date	Description
January 20, 2025	The new leadership team arrived at OPM.
January 24, 2025	A test email was sent to all federal employees requesting a response. It appears that the GWES was operational on this date because the system was sending and receiving emails.
January 26, 2025	A second test email was sent to all federal employees.
January 28, 2025	The “Fork in the Road” email was sent to all federal employees requesting a response if the employee decides to participate in a deferred resignation program.
February 22, 2025	The “What did you do last week?” email was sent to all federal employees requesting that employees respond with five bullets of what they accomplished the previous week and copy their manager. Five bullets have been requested weekly since this initial email.

APPENDIX II

OPM's August 14, 2025, response to the draft flash report issued August 4, 2025:

Recommendation 1.

We recommend that OPM retroactively follow its established ECM process and submit the GWES to the Change Review Board and Engineering Review Board to conduct a security, compliance, and technical specifications analysis to ascertain the impact on OPM's network and remediate any control weaknesses that are found.

OPM Response.

Non-Concur. The purpose of the ECM process is to ensure that any proposed changes are elevated at a sufficiently high level within CIO. The Change Review Board and Engineering Review Board may only make non-binding recommendations to the OPM CIO. In all cases, however, the CIO remains the ultimate decision-maker.

In this instance, the CIO directly approved the change to add the GWES system after careful consideration of the impact on OPM's network. He did so in consultation with OPM's Acting Director, who had personal experience building the Enterprise Human Resources Integration (EHRI) system as a supervisor at OPM. Both the CIO and the Acting Director concurred that an ECM process was not required. GWES was an outgrowth of EHRI that merely provided a mechanism to email many government employees at once using the OPM Azure Communication Service (ACS).

While the ECM process can serve a valuable function, it is not required in all instances. Technological systems must be agile and responsive to rapidly-evolving government needs—not captive to inflexible bureaucratic processes. In the first part of 2025, there was an urgent need to rapidly communicate with government employees regarding important workforce initiatives like the Trump Administration's Deferred Resignation Offer, 5 Bullets, and other workforce optimization initiatives. Using existing systems and technologies whose purpose is to facilitate efficient human capital management to perform what would be considered an entirely routine task (emailing all employees at once) at most any other enterprise in response to an urgent need did not require a complicated change management process.

In any event, prior to receipt of this draft report, OPM's Director determined that the need for the "5 Bullets" program had ended and notified all OPM employees as well as other federal agencies of this determination last week. As a result, OPM has decommissioned the GWES; therefore, OPM cannot concur.

Recommendation 2.

We recommend that OPM accurately classify the GWES in accordance with the OPM Security Authorization Guide.

OPM Response.

Non-Concur. GWES was correctly determined to be an outgrowth of the EHRI system which could be covered under the same ATO. EHRI is a database that is designed to be used by OPM for governmentwide workforce management and planning. Its name gives away its purpose-Enterprise Human Resources Integration. EHRI integrates data from agency payroll systems and makes it usable for OPM to drive efficient and effective workforce planning. EHRI is the authoritative data store of email addresses, and GWES used that store to establish as an official government-wide communication channel to allow the Executive Branch to communicate rapidly and efficiently with its employees regarding important workforce initiatives. Thus, both systems fall within the same mission/business process under NIST 800-39 Tier 2. OMB A-130 specifies agencies have significant flexibility in determining what constitutes an information system and its associated boundary. Across government, it is a common practice to combine multiple related applications into a single ATO.

Finally, prior to receipt of this draft report, OPM's Director determined that the need for the "5 Bullets" program had ended and notified all OPM employees as well as other federal agencies of this determination last week. As a result, OPM has decommissioned the GWES; therefore, OPM cannot concur.

Recommendation 3.

We recommend that OPM initiate an ATO for the GWES as a result of the reclassification outlined in recommendation 2. The ATO should include security categorization, control selection, implementation, and assessment.

Note – if the reclassification of GWES determines that it is a subsystem of another OPM system, a reauthorization of the selected parent system should be conducted.

OPM Response.

Non-Concur. As stated in OPM's response to Recommendation 2, there was no need for a separate ATO for the GWES system. Therefore, OPM cannot concur.

Recommendation 4.

We recommend that OPM immediately take appropriate steps to determine whether sensitive and/or classified information is stored by the GWES or disseminated to other agencies. Furthermore, if any sensitive and/or classified information is stored or has been disseminated by the GWES take immediate steps to ensure data security and privacy.

OPM Response.

Non-Concur. OPM recognizes the importance of ensuring data security and privacy. Therefore, OPM sent clear instructions not to send any classified information, links, attachments, or any sensitive PII. GWES has been decommissioned and there is no continuing need to maintain the records in that system. In his memo to the OPM Director, the CIO has already taken appropriate steps. Therefore, this recommendation should be closed.

Recommendation 5.

We recommend that OPM develop and implement policies, procedures, and controls for handling potentially sensitive and/or classified information received by the GWES.

OPM Response.

Non-Concur. Please refer to OPM's response to Recommendation 4. This recommendation has been superseded by the decommissioning of the GWES system.

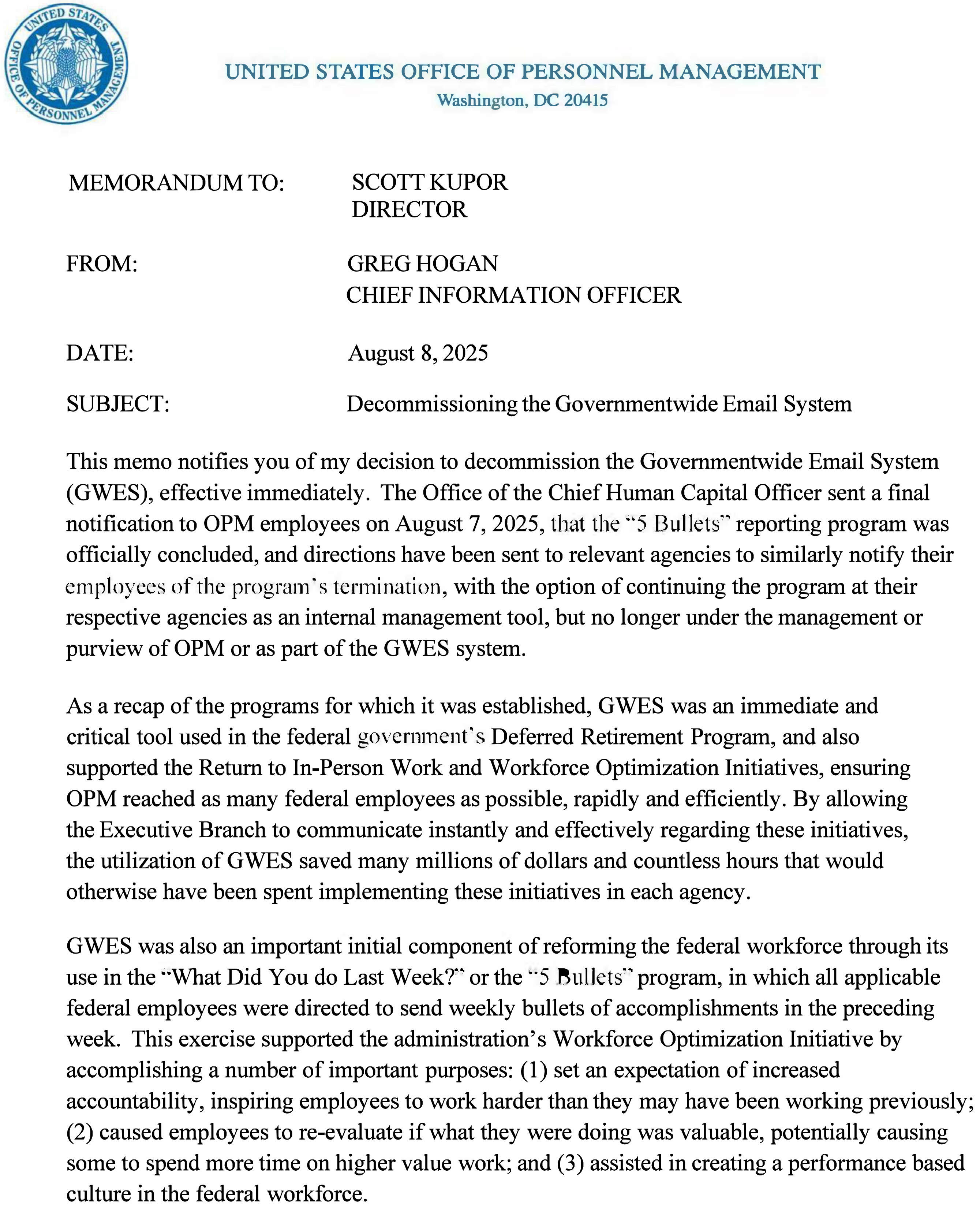
Recommendation 6.

We recommend that OPM address the deficiencies in its audit engagement process and procedures to ensure consistent and efficient access to personnel and information in support of OIG audits.

OPM Response.

Concur in principle. OPM appreciates the concern OIG expresses for this issue and the importance of an effective and efficient audit engagement process. OPM recently changed the delegation for incoming audits in order to centralize the intake of these matters and inform the appropriate parties. OPM acknowledges that there were some unique delays because of the change from a Risk Assessment to an Audit, and as a result of instituting response protocols with new personnel. OPM will consider take additional appropriate steps to ensure that OPM processes and procedures provide timely support to OIG audits.

APPENDIX III



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

MEMORANDUM TO: SCOTT KUPOR
DIRECTOR

FROM: GREG HOGAN
CHIEF INFORMATION OFFICER

DATE: August 8, 2025

SUBJECT: Decommissioning the Governmentwide Email System

This memo notifies you of my decision to decommission the Governmentwide Email System (GWES), effective immediately. The Office of the Chief Human Capital Officer sent a final notification to OPM employees on August 7, 2025, that the "5 Bullets" reporting program was officially concluded, and directions have been sent to relevant agencies to similarly notify their employees of the program's termination, with the option of continuing the program at their respective agencies as an internal management tool, but no longer under the management or purview of OPM or as part of the GWES system.

As a recap of the programs for which it was established, GWES was an immediate and critical tool used in the federal government's Deferred Retirement Program, and also supported the Return to In-Person Work and Workforce Optimization Initiatives, ensuring OPM reached as many federal employees as possible, rapidly and efficiently. By allowing the Executive Branch to communicate instantly and effectively regarding these initiatives, the utilization of GWES saved many millions of dollars and countless hours that would otherwise have been spent implementing these initiatives in each agency.

GWES was also an important initial component of reforming the federal workforce through its use in the "What Did You do Last Week?" or the "5 Bullets" program, in which all applicable federal employees were directed to send weekly bullets of accomplishments in the preceding week. This exercise supported the administration's Workforce Optimization Initiative by accomplishing a number of important purposes: (1) set an expectation of increased accountability, inspiring employees to work harder than they may have been working previously; (2) caused employees to re-evaluate if what they were doing was valuable, potentially causing some to spend more time on higher value work; and (3) assisted in creating a performance based culture in the federal workforce.

Upon conferring with the key officials of these programs, I have confirmed that these purposes have served their short-term value of initiating a desired reset to federal workforce managers and employees, and that the GWES may now be properly decommissioned. As part of the close out procedures, I will following all applicable OCIO protocols for decommissioning the GWES system.

It is my understanding that copies of email records in the GWES system have fully served their purpose because any needed records are scheduled on various other National Archives and Records Administration (NARA) General Records Schedules (GRS), under appropriate records retention periods, and are no longer needed for retention in GWES. For example, some of the records in GWES are “intermediary records,” which have been utilized in creating subsequent official records, such as in employee eOPFs, retirement records, or in supervisor or employee working files (GRS 2.2, Employee Management Records); or are “ transitory records ” records of short-term value, generally retained for less than 180 days (GRS 5.2, Intermediary or Transitory Records). Certain senior officials of the agency have their email records scheduled under GRS 6.1, Capstone records, and those records are also no longer needed in the GWES system.

Therefore, and in light of all of the above, in addition to decommissioning the GWES system, I will also authorize the appropriate officials to dispose of all copies of the records in the GWES system in accordance with any relevant NARA guidance for disposal of electronic records.

Finally, I note that mass emailing of federal employees has been used previously as a strategy for efficient governmentwide federal employee communications, such as for Federal Employee Viewpoint Survey distribution. Indeed, it is crucial that the President be able to manage the Executive Branch as a single workforce driving towards a common mission: serving the American people. This includes rapidly communicating on key workforce initiatives.

Going forward, OPM will continue to explore ways to allow Executive Branch leadership to communicate instantly with all federal employees, to maximize the efficient management of the workforce – consistent with the Congress’s requirement in the Civil Service Reform Act of 1978 that the Executive Branch demand the highest standards of employee performance” and work towards “the continued development and implementation of modern and progressive work practices to facilitate and improve employee performance and the efficient accomplishment of the operations of the Government.”

Greg Hogan

Digitally signed by Greg Hogan
Date: 2025.08.08
01:34:01 -04'00'

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: https://oig.opm.gov/contact/hotline

By Phone: Toll Free Number: (877) 499-7295

By Mail: Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100