epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

VIA EMAIL

February 14, 2025

U.S. Office of Personnel Management
1900 E St., N.W.
OPIM/FOIA Room 5H35
Washington, D.C. 20415-7900
FOIA@opm.gov
202-606-3642

Freedom of Information Act Request

Dear FOIA Officer:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Office of Personnel Management ("OPM").

EPIC seeks documents related to the security of databases, information, and information systems maintained by OPM.

Documents Requested

EPIC requests disclosure of the following documents:

1. Requests for access privileges to OPM databases and IT systems made or received by OPM's Office of the Chief Information Officer between January 20, 2025, and the date on which this request is processed, including but not limited to requests made via email and Microsoft Teams.
2. The Security Assessment Report ("SAR") created to assess the security risks of establishing the Government-Wide Email System at OPM.
3. The authorization to operate ("ATO"), also known as authority to operate, granted to operate the Government-Wide Email System at OPM.

Background

Each executive agency, including OPM, staffs a Chief Information Officer ("CIO") tasked with providing a sound, secure, and integrated information technology architecture that is monitored for efficiency and effectiveness. 40 U.S.C. § 11315(b), (c). OPM's Chief Information Officer is Greg Hogan, a former AI company executive in his first government position.[1] As

[1] Natalie Alms, *OPM Reveals New Details About Its CIO*, Nextgov/FCW (Feb. 12, 2025), https://www.nextgov.com/people/2025/02/opm-reveals-new-details-about-its-cio/402955/.

OPM's Chief Information Officer, Greg Hogan heads up the agency's Office of the Chief Information Officer ("OCIO"). Prior to Greg Hogan, the position of OPM CIO was held by Melvin Brown II.[2] The OCIO processes requests for access to databases maintained by the OCIO.

Generally, all federal information and information systems follow the Risk Management Framework ("RMF") developed by the National Institute of Standards and Technology ("NIST"). Federal Information Security Management Act, 44 U.S.C. § 3554(a)(1)(B)(i). The RMF requires agencies to conduct Security Control Assessments that implement organization-approved Security Assessment Plans.[3] The results of the assessment plans must be produced in a Security Assessment Report ("SAR").[4] Following the assessment, a senior official decides whether to authorize the system to operate.[5] This is known as an Authorization to Operate, Authority to Operate, or ATO.

A government agency's email server is an information system within the meaning of FISMA. *See* 44 U.S.C. § 3502(6), (8). Beginning on January 23, 2025, OPM began operating a government-wide email server,[6] later dubbed the Government-Wide Email System.[7] This server has been used by the associates of Elon Musk and the DOGE/USDS team to simultaneously contact all federal employees.[8] Before installing and using this email server, OPM was required to follow the RMF, including developing a SAR and obtaining an ATO.

Request for Waiver of Fees

EPIC is a "representative of the news media" for fee classification purposes. *EPIC v. DOD*, 24 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested records with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II); 5 C.F.R. § 294.109(c). Any further fees should be waived because the disclosure of the documents requested is in the public interest, "likely to contribute significantly to public understanding of the operations or activities of the Government," and not in the commercial interest of EPIC, the requester. 5 C.F.R. § 294.109(f).

---

[2] Madison Alder, *Melvin Brown II Swapped Out as OPM's Chief Information Officer*, FedScoop (Jan. 22, 2025), https://fedscoop.com/melvin-brown-ii-swapped-out-opm-chief-information-officer/.
[3] U.S. Department of Commerce & NIST, NIST SP 800-53A, *Assessing Security and Privacy Controls in Information Systems and Organizations* (Jan. 2022), https://doi.org/10.6028/NIST.SP.800-53Ar5.
[4] *Id*.
[5] NIST, Risk Management Framework (RMF) – Authorize Step, csrc.nist.gov, https://csrc.nist.gov/Projects/risk-management/about-rmf/authorize-step.
[6] *See* Federal Government-Wide Email Communication Test, OPM.gov (Jan. 23, 2025), https://www.opm.gov/statements/federal-government-wide-email-communication-test-coming/.
[7] Riccardo Biasini, *Privacy Impact Assessment for Government-Wide Email System (GWES)*, OPM (Feb. 5, 2025), https://www.opm.gov/media/kfpozkad/gwes-pia.pdf.
[8] A.J. Vicens, *Email Server Used by Elon Musk's Team Does Not Pose Privacy Risk, Agency Says*, Reuters (Feb. 5, 2025), https://www.reuters.com/world/us/controversial-opm-email-server-operates-entirely-government-computers-agency-2025-02-05/.

First, the documents requested are in the public interest. *Id*. As discussed above, OPM is required to follow a framework that ensures the security of the government, its employees, and any individuals who may correspond with it. The RMF is a critical piece of protecting American infrastructure. Further, OPM receives requests from external personnel attempting to access information systems maintained by OPM. The documents requested will give insight into how OPM is safeguarding its information and information systems. The public has an interest in learning how OPM is conducting its security practices.

Second, the documents requested are "likely to contribute significantly to public understanding of the operations and activities of the Government." *Id*. This request seeks documentation that will shed significant light on OPM's security practices, activities of security-involved personnel, and the safety of the information systems maintained by OPM. The requested documents will give the public significant insight into the security practices of OPM and its OCIO. Therefore, disclosure of these documents will "contribute significantly to the public understanding of the operations and activities of the Government." *Id*.

Third, the documents requested are not in EPIC's commercial interest. EPIC is a non-profit organization committed to privacy, open government, and civil liberties. As a non-profit research organization, EPIC has no commercial interest in the requested information. Therefore, as demonstrated above, EPIC is a news media requester and satisfies the public interest standard under 5 C.F.R. § 294.109(f).

For these reasons, a fee waiver should be granted.

Request for Expedited Processing

EPIC is entitled to expedited processing of this request under the FOIA and OPM's public FOIA guidance. 5 U.S.C. § 552(a)(6)(E)(v)(II); *Freedom of Information Act: Reference Guides*, OPM.gov, https://www.opm.gov/information-management/freedom-of-information-act/#url=Guides (last visited Feb. 13, 2025).

First, EPIC is entitled to expedited processing of its request because it is primarily engaged in disseminating information to the public. Again, EPIC is a nonprofit research center and news media representative. EPIC routinely publishes reports[9] and helpful blog posts[10] concerning privacy and civil liberties issues. As such, EPIC is primarily engaged in disseminating information to the public.

Second, the documents requested are urgently needed to inform the public concerning actual or alleged Federal Government activity. As discussed in the Background section, OPM should have created an SAR and received an ATO prior to installing and using a new email server. OPM is currently involved in litigation concerning this email server and the agency's

[9] *See, e.g.*, EPIC, *Generating Harms*, EPIC.org, https://epic.org/generating-harms/ (last visited Jan. 28, 2025).
[10] *See* EPIC, *Analysis*, EPIC.org, https://epic.org/analysis/ (last visited Jan. 28, 2025).

practices safeguarding the information it maintains in other systems.[11] The documents requested will inform the public on the Federal Government's activity.

EPIC certifies that the above is true and correct.

Conclusion

Thank you for your consideration of this request. EPIC anticipates your response to its request within ten (10) calendar days. 28 C.F.R. § 16.5(e)(4). For questions regarding this request, please contact Abigail Kunkler, kunkler@epic.org, cc: foia@epic.org.

Respectfully submitted,

/s Abigail Kunkler
Abigail Kunkler
EPIC Law Fellow

[11] *See, e.g.*, Billy Mitchell, *Lawsuit Claims Systems Behind OPM Governmentwide Email Blasts Are Illegal, Insecure*, FedScoop (Jan. 28, 2025), https://fedscoop.com/opm-email-federal-workforce-lawsuit-server-privacy-security/.