UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

March 15, 2023

MEMORANDUM

SUBJECT: Management Implication Report Concerning Vulnerabilities to EPA OIG Information Security and Oversight Independence

FROM: Jason Abend, Assistant Inspector General
Office of Investigations

Abend, Jason Digitally signed by Abend, Jason Date: 2023.03.15 13:42:14 -04'00'

TO: Vaughn Noga, Chief Information Officer and Deputy Assistant Administrator for Environmental Information
Office of Mission Support

Purpose: The U.S. Environmental Protection Agency Office of Inspector General identified vulnerabilities related to the EPA's network structure, specifically, the Microsoft Office 365, or O365, environment in which little or no network segmentation exists between the EPA proper and the OIG. The EPA's O365 administrators can modify OIG account settings as well as access and view sensitive data within the O365 environment without the knowledge or input of the OIG, including email and other data of senior OIG employees and sensitive shared email inboxes. Additionally, poor user access controls and limited event logging degrade the OIG's ability to determine details about user activity within the O365 environment.

Background: On April 8, 2022, the EPA OIG Office of Investigations learned that an EPA Criminal Investigation Division, or CID, special agent was improperly granted access to the OIG's whistleblower protection coordinator email account, Whistleblower_Protection@epa.gov, which is hosted on the EPA's O365 environment. On April 14, 2022, the OIG initiated an investigation to determine the facts of the allegation. Because the OIG opened an investigation and the access was determined to be limited to within the Agency, the OIG did not report the issue under the Agency breach procedure.[1] The OIG was made aware that the Office of Criminal Enforcement, Forensics and Training reported the issue to the Computer Security Incident Response Capability on June 17, 2022.

The whistleblower email account is a shared mailbox that was created to receive correspondence from individuals seeking additional information about whistleblower protections afforded under federal law and other governing regulations. The whistleblower email account should only be accessed by OIG employees designated as the whistleblower protection coordinator or alternate. Generally, this role is performed by attorneys from the OIG's Office of Counsel. The whistleblower email account was not

[1] *Responding to Personally Identifiable (PII) Information Breach Procedure,* Directive No. CIO 2151-P-02.4, dated November 19, 2020, states that congressional notification would only be triggered by a "major incident," defined as "[a]ny incident that is likely to result in demonstrable harm to the national security interests, the Agency, foreign relations or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people." *Id*. at 29.

designed to receive and process whistleblower complaints, as this function is fulfilled by the OIG Hotline. Despite its intended use, however, the whistleblower email account has occasionally received whistleblower complaints and complaint-related information. Since its creation in 2014, an estimated 20 to 25 individuals per year made a disclosure, sought information about whistleblower protections, or reported retaliation. These whistleblower disclosures were made by EPA and non-EPA employees who may have misunderstood how to properly report whistleblower complaints. Aside from occasionally receiving complaint information, the whistleblower email account, by virtue of its intended function of providing whistleblower protection information, can be reasonably expected to contain the identifying information of EPA employees who were considering, or had already initiated, a confidential whistleblower complaint.

Through investigative activity, the OIG concluded that on or about April 6, 2022, the whistleblower protection coordinator discovered additional network users were assigned permission to access the whistleblower email account. The coordinator determined that all users with access permissions were former whistleblower protection coordinators except one. It was determined that the one user whose name was not familiar to the coordinator was a CID special agent. After the whistleblower coordinator determined that the user was not employed by the OIG and had no reason to access the whistleblower email account, the unauthorized access was reported to the Office of Investigations.

This issue initially arose when a CID special agent's supervisor directed that special agent to gain access to the shared mailbox that is used to receive and review a specific category of whistleblower complaints. The CID maintains a relationship with a partner federal agency, whereby it provides the CID with investigative leads from the complaints it receives.

Definitions

Security Groups: Groups that are used to grant access to Microsoft 365 resources, such as SharePoint. These groups can make administration easier than adding users to each resource individually.

Shared mailbox: A mailbox that multiple users can use to read and send email messages.

Superuser: A user who is authorized, and therefore trusted, to perform security-relevant functions that ordinary users are not authorized to perform.

When the CID special agent contacted EPA information technology support, they requested access to a "whistleblower email box" without specifying the exact name of the shared mailbox. Because the OIG's whistleblower email account is the only whistleblower-related shared mailbox in the EPA directory, the CID special agent was granted access to that OIG email account on or about September 13, 2021, despite not being an authorized user of that shared inbox. The EPA IT specialist who granted access was an EPA contracted employee assigned to the Office of Mission Support.

Based on available information, it is likely that the CID special agent maintained access to the whistleblower email account until around December 2021. For about three months, the CID special agent had complete access to the account and its contents, including the privileged names of whistleblowers, potential whistleblowers, and EPA employees named as the subject of complaints. During the course of this investigation, the OIG interviewed the CID special agent about the access to the whistleblower email account. The CID special agent stated that the contents of the whistleblower email account were not consistent with what they expected. The CID special agent further explained that this led them to share their screen with their supervisor to inquire what they should be doing with the emails. At that time, the supervisor confirmed that the CID special agent was not viewing the correct inbox and needed to call IT to have the inbox uninstalled and the correct inbox installed. Subsequently, the special agent notified the IT help desk to remove the inbox immediately. The special agent stated that they did not view much of the inbox, nor did they have any recollection of any details, sensitive or otherwise, contained in any of the emails viewed. The special agent further stated that other than their supervisor, they had not shown anyone the information contained in the whistleblower email account. The special agent also confirmed that they did not share the details of the emails they viewed.

Concerns Identified: In accordance with the Inspector General Act of 1978, as amended, the independence of the inspector general from the parent agency is a critical component to executing the oversight mission of each OIG. Additionally, the Whistleblower Protection Act, as amended, provides confidentiality for whistleblowers making disclosures concerning their workplace. In this case, the problems identified within this Management Implication Report create serious concern for the OIG's ability to maintain independence and ensure confidentiality for whistleblowers within the current construct of the network space shared between the OIG and the EPA.

The EPA IT specialists assigned to the Office of Information Technology Operations, within the Office of Mission Support, serve as administrators of the O365 environment with broad access to nearly all EPA and OIG email accounts administered through the O365 environment, including OIG shared mailboxes like the whistleblower email account and other sensitive accounts. Additionally, the O365 administrators maintain broad access to administer other subapplications of the O365 environment, including Microsoft Teams. These O365 administrators are EPA employees or contractors who, by default, have almost unfettered access to all accounts within the O365 environment. Because of this "superuser" level of access, these EPA employees and contractors could access nearly any sensitive OIG data held within the O365 environment, including the Microsoft Outlook and Teams data of senior OIG employees or sensitive mailboxes like the whistleblower email account. Additionally, the OIG's IT specialists do not possess the same superuser level of access to the O365 environment, resulting in the OIG's IT specialists relying on EPA O365 administrators to make administrative changes to OIG user accounts.

Initial investigative steps to retrieve O365 event logs from the Office of Information Technology Operations showed that O365 event logs were not adequately maintained by the EPA, making it impossible to use such event logs to determine when changes were made to the whistleblower email account and by which users. Because of the voids in the event logs, there was no digital evidence to determine which EPA O365 administrator provided access to the whistleblower email account. Due to insufficient event log preservation, future determinations regarding which users took which action within the O365 environment would also be difficult to determine. This presents a concern for OIG independence given the superuser-level that EPA O365 administrators possess that allows their access to OIG accounts across the O365 environment.

In the case of shared mailboxes within the O365 environment, the EPA employs an additional user access safeguard known as security groups, but this measure does not adequately protect access to OIG accounts in the O365 environment, like the whistleblower email account. Security groups are established and associated with a shared mailbox, essentially acting as a user access control list. Users, including trusted users, are added to the security group account and may access the associated shared mailbox. Despite this additional access control, the default superuser-level access granted to O365 administrators allows them to access all OIG accounts within the O365 environment, including the OIG's sensitive shared email accounts such as the whistleblower email account, even if they are not assigned to the associated security groups. This allows these EPA employees and contractors to access nearly any sensitive OIG data held within the O365 environment.

Prior to May 2022, EPA IT specialists serving as O365 administrators would routinely grant users access to shared mailboxes without conducting additional verification to confirm that the requesting user required access. Similarly, only specific O365 accounts of senior EPA employees, including the EPA administrator's email account, were afforded additional safeguards. The additional safeguard to senior EPA employee accounts was simply a directive among EPA IT specialists to receive permission before making any changes to the account or allowing other users access to the account. The EPA IT specialists interviewed by the OIG were unaware of any similar safeguards for granting access to sensitive OIG

accounts, including that of the inspector general. The Office of Mission Support released a policy memorandum in May 2022 that directed IT specialists to forward any shared mailbox access requests to the designated mailbox owner before granting access to the account. While the policy sought to impose an additional security measure, the policy change did not practically curb the unimpeded access that the EPA O365 administrators have to OIG employee accounts.

In June 2022, the OIG and the Office of Mission Support discussed a potential solution to the issue of EPA O365 administrators having unlimited access to OIG accounts. The OIG suggested providing OIG IT specialists with sole access to administer the OIG accounts within O365. Additionally, the OIG suggested segmentation of OIG accounts within the O365 environment to prevent EPA employees from being able to access or modify those accounts. As of the date of this report, the OIG had not received a response from the Office of Mission Support regarding a complete transfer of administrator access for all OIG email accounts within O365. Meanwhile, the OIG transferred control of our confidential and sensitive shared email accounts to OIG email administrators. The shared email accounts that are now under OIG administrator control are the whistleblower protection coordinator, OIG Hotline, Freedom of Information Act, information systems officer, and OIG Counsel mailboxes. Additionally, two OIG IT specialists review the account audit reports for those shared accounts on a weekly basis to ensure the integrity of access lists and authorized users.

My office is notifying you of this issue so that the Agency may take whatever steps it deems appropriate. If you decide it is appropriate for your office to take or plan to take action to address these matters, the OIG would appreciate notification of that action. Should you have any questions regarding this report, please contact Special Agent in Charge [redacted] at [redacted].

cc: Janet McCabe, Deputy Administrator
Dan Utech, Chief of Staff, Office of the Administrator
Sean W. O'Donnell, Inspector General
Kimberly Patrick, Principal Deputy Assistant Administrator for Mission Support