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

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

December 9, 2021

MEMORANDUM

SUBJECT: Management Implication Report: [redacted] Allowing Remote Access to Threat Actors

FROM: Marc Perez, Acting Assistant Inspector General
Office of Investigations
Marc A. Perez Digitally signed by Marc A. Perez Date: 2021.12.09 13:09:33 -08'00'

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

Purpose: The U.S. Environmental Protection Agency's Office of Inspector General has identified a critical vulnerability concerning software installations on EPA-furnished computers: [redacted].[1] While information security oversight is the responsibility of the EPA Office of Mission Support, the OIG has identified several instances of unknown third-party threat actors accessing EPA-furnished computers [redacted]

Background: The OIG initiated several investigations after being notified by the EPA's Computer Security Incident Response Center that threat actors had accessed EPA computers—and by proxy, the EPA network—via malicious [redacted]

The following are brief synopses of recent OIG investigations that identified this type of attack as the primary means of attack:

- In January 2021, an EPA employee received a malicious [redacted] for [redacted] on the employee's EPA-furnished computer. [redacted]"[2]

[1] [redacted]

[2] [redacted].

- In February 2021, an EPA employee located a malicious [redacted] website. [redacted]
- In July 2021, an EPA employee received a malicious [redacted] on the employee's EPA-furnished computer. [redacted]
- In August 2021, an EPA employee received a malicious [redacted] on the employee's EPA-furnished computer [redacted]

Problems Identified: [redacted] OIG continues to investigate what information, if any, the threat actors reviewed or exfiltrated from the affected EPA-furnished computers.

The OIG is continuing its investigation into these matters. Based on the details above, however, my office is notifying you of [redacted], so that the Agency may take whatever steps, if any, it deems appropriate to ensure that EPA networks, systems, and information are safeguarded from nefarious actors [redacted]. The OIG would appreciate notification of any actions the Agency takes to address these matters.

Should you have any questions regarding this report, please contact [redacted] or me at (202) 603-4861.

cc: Sean W. O'Donnell, Inspector General
Janet McCabe, Deputy Administrator
Dan Utech, Chief of Staff, Office of the Administrator
Lynnann Hitchens, Acting Principal Deputy Assistant Administrator Performing Delegated Duties of Assistant Administrator, Office of Mission Support