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

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

September 7, 2021

MEMORANDUM

SUBJECT: Management Implication Report: Failure to Follow Agency Procedure to Report Cyber Incident

FROM: Helina Wong, Assistant Inspector General
Office of Investigations

HELINA WONG
Digitally signed by HELINA WONG
Date: 2021.09.07 09:08:45 -04'00'

TO: Ted Stanich, Associate Administrator
Office of Homeland Security

Purpose: The U.S. Environmental Protection Agency's Office of Inspector General has identified a failure to follow Agency procedure—specifically EPA Classification No. CIO 2150-P-08.2, *EPA Information Procedure, Information Security – Incident Response Procedures*—concerning reporting and response requirements for cybersecurity incidents. The failure to follow this procedure occurred after EPA employees were notified of a potential data breach of EPA information related to the EPA Facility Registry Service, or FRS.

Background: On June 9, 2021, a U.S. government law enforcement agency external to the EPA notified the OIG [redacted]

Separately, on June 10, 2021, the EPA Office of Homeland Security informed the OIG via email that it had notified the Federal Bureau of Investigation, the U.S. Department of Homeland Security, and the National Security Agency of a potential EPA data breach. EPA OHS coordinated with external law enforcement, intelligence, and cybersecurity agencies prior to notifying OIG and the CSIRC of the incident. The OIG subsequently contacted the FBI Cyber Division and advised them that the incident was not a data breach as originally reported. Further, a review of embedded email communication in the EPA Office of Homeland Security's notification to the OIG revealed that the Cable News Network (CNN) attempted to obtain information about the incident from EPA Press Secretary [redacted].

ECD Capabilities: Early notification of a potential data breach, cyber intrusion, or other cyber event is critical to ensuring the integrity of EPA's cyber infrastructure. The EPA OIG has a dedicated Electronic Crimes Division that is staffed with criminal investigators who are specially trained to investigate cases like these. As we mentioned in our recent Management Implication Report, *Management Implication Report Concerning Lack of Information Security Protection of Off-Network EPA Device*, it is crucial that we are involved early in any cyber investigation. This is because these specially trained criminal investigators have a unique set of tools that allow them to collect and analyze electronic and cyber evidence before it is lost. The EPA OIG also has existing relationships with a broad array of external law enforcement through formal arrangements, such as participation in FBI cyber task forces, and informal arrangements, such as with other IG investigative offices. These relationships allow the EPA OIG to quickly identify which external law enforcement partners to contact and who the appropriate points of contact are at those partners.

Problems Identified: Agency personnel did not follow the EPA procedure outlined in EPA Classification No. CIO 2150-P-08.2, *EPA Information Procedure, Information Security – Incident Response Procedures*, Section 6, Subsection IR-6, "Incident Reporting," paragraph 2(b)(i), which states:

> The OIG shall serve as the primary point of contact for coordination with law enforcement agencies in regards to incident reporting. Any contact with law enforcement agencies shall be coordinated through the OIG.

Additionally, section 8, "Roles and Responsibilities," states, in part:

> OIG-OI has the following responsibilities with respect to incident response:
> a) Determine if an incident identified by CSIRC as possibly criminal in nature is actually criminal in nature.
> b) Serve as the primary point of contact for coordination with law enforcement.
> c) Conduct criminal investigations of incidents when criminality is determined.
> d) Assist CSIRC and ISO in forensic capabilities, when possible and needed.

Specifically, EPA OHS failed to adhere to this requirement when it contacted law enforcement agencies external to the EPA. Because these personnel did not immediately report the incident to the CSIRC or the OIG, the OIG was not made aware of critical information needed to identify and mitigate threats, as alleged, to EPA information systems. Because the incident, as alleged, constituted a violation of 18 U.S.C. Section 1030, *Fraud and related activity in connection with computers,* EPA personnel should have reported the incident to the OIG immediately after becoming aware of the potential breach. EPA OHS coordination with the FBI, a law enforcement agency, violated this procedure, as the office did not coordinate reporting the incident with the OIG, as required.

Any potential harm from failure to adhere to EPA procedure was, in this instance, mitigated by the OIG's early assessment that the reported data breach did not contain sensitive or personally identifiable information. Adhering to EPA procedure is important, however, because early coordination with the OIG on reported data breaches prevents sensitive law enforcement or erroneous information from potentially being disseminated to the media, which could cause

damage to the Agency's systems, operations, programs, or personnel, or to the investigation, or erode the public's trust in EPA programs, operations, and data dependent upon information security.

The OIG is continuing its investigation into this matter. Based on the details above, my office has identified this incident as a failure to follow EPA procedure and is notifying you so that the Agency may take whatever steps it deems appropriate to ensure that cyber incident response procedures, including prompt reporting to the OIG, are followed by all EPA employees.

Should you have any questions regarding this report, please contact Special Agent-in-Charge [redacted] at [redacted] or me at (202) 566-2841.

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