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

OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

July 9, 2021

MEMORANDUM

SUBJECT: Management Implication Report Concerning Lack of Information Security Protection of Off-Network EPA Device

FROM: Helina Wong, Assistant Inspector General
Office of Investigations
HELINA WONG Digitally signed by HELINA WONG Date: 2021.07.09 11:12:29 -04'00'

TO: Jennifer Orme-Zavaleta, Acting Assistant Administrator and EPA Science Advisor
Office of Research and Development

Purpose: The U.S. Environmental Protection Agency's Office of Inspector General has identified a critical control issue concerning the information security and scientific integrity of the [redacted] an environmental air sensor device operated by the Office of Research and Development's Center for Environmental Measurement and Modeling's Air Methods and Characterization Division. The OIG discovered this issue when [redacted] made us aware of a security breach of one [redacted] device in [redacted] wherein access to the device was restricted after an unknown threat actor gained remote access to it, created a password, and encrypted the contents of the device. The OIG believes that, based on the details of this attack, the device was attacked by ransomware. This memorandum addresses the potential lack of safeguards on remote devices procured, implemented, and operated by the ORD. It also addresses scientific integrity concerns with respect to data collected from devices such as these when no access controls to the device are implemented. Lastly, this memorandum serves as a reminder that EPA employees must report all cyber-intrusion incidents to the OIG, consistent with the Inspector General Act of 1978, as amended, and EPA policy.

Background: On April 23, 2021, ORD employees attempted to remotely log into the [redacted] device and were denied access. ORD employees eventually gained access and discovered that the contents of the device were encrypted and not accessible. The ORD then contacted [redacted] the manufacturer of the [redacted] device, who assisted the ORD with wiping [redacted] on the [redacted] device. On April 27, 2021, the ORD notified [redacted] of the incident.

Problems Identified: Inadequate access controls combined with the [redacted] device being connected to the internet likely enabled external access to the device by unknown threat actors. The ORD attempted to notify [redacted] on April 23, 2021, but emailed the incorrect address, precluding notification of the incident until April 27, 2021. Unfortunately, due to EPA incident responders not being permitted to examine the device after it was attacked and due to [redacted] remediating the device by completely wiping it without preserving any data, evidence that could have supported an investigation into the attack no longer exists. After reviewing the email correspondence provided to [redacted] from the ORD, the OIG discovered that a password was not set on the [redacted] device. Further, the [redacted] device was connected to the open internet using an "air card," which is an appliance used to provide an internet connection over

cellular signal. The means by which this device was accessed by the ORD may indicate a pattern of inadequate information security across devices located off the EPA's Agency network. With the lack of access controls, guarantees of scientific integrity cannot be made as the [redacted] devices do not appear to include or require a password. Programs that the [redacted] devices support may thus be receiving flawed data, skewing programs and studies used to support further EPA research and funding. Further, there is a potential threat for malicious software to be inadvertently downloaded or pushed from a malicious source to devices lacking security. Such malicious software could create a vulnerability beyond the [redacted] devices themselves or render the devices completely inoperative.

The OIG continues its investigation into this matter. Based on the foregoing results, my office has identified this as a critical control issue, so that the Agency will take whatever steps it deems appropriate to ensure the integrity of vital scientific research conducted by the ORD.

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

cc: Sean W. O'Donnell, Inspector General
Dan Utech, Chief of Staff, Office of the Administrator
Donna Vizian, Acting Assistant Administrator for Mission Support
Vaughn Noga, Deputy Assistant Administrator for Environmental Information and Chief Information Security Officer, Office of Mission Support