

CUI//PRIVILEGE

Management Implication Report: Unauthorized Use of Software on EPA Computers

September 22, 2025 | Report No. 25-N-0049



REDACTED VERSION FOR PUBLIC RELEASE

The full version of this report contained controlled unclassified information. This is a redacted version of that report, which means the controlled unclassified information has been removed. The redactions are clearly identified in the report.






OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

September 22, 2025

MEMORANDUM

SUBJECT: Management Implication Report: Unauthorized Use of Software on EPA Computers

FROM: Nic Evans, Acting Assistant Inspector General
Office of Investigations 

TO: Carter Farmer, Chief Information Officer and Deputy Assistant Administrator
for Information Technology and Information Management
Office of Mission Support

PURPOSE AND OVERVIEW: The U.S. Environmental Protection Agency Office of Inspector General has identified concerns regarding the installation and use of unauthorized software, specifically juggler software, on EPA computers and networks. Commonly referred to as “mouse jigglers,” juggler software simulates activity on a laptop, preventing the laptop from entering sleep mode and locking out its user. The EPA has a clear, consistent, and uniform policy that prohibits the download, installation, and execution of unauthorized software on the Agency’s computers and networks. EPA policy also requires unauthorized software to be immediately removed upon detection. Furthermore, the EPA uses several tools to enforce this policy, including Microsoft Windows Installer to prevent the installation of unauthorized software and network scans to detect the presence of unauthorized software.¹

The EPA has not authorized any juggler software for any use on its computers or systems. After running network scans in two EPA regions in November and December 2024, however, the Agency discovered 120 employees and contractors using juggler software. Our investigation found that juggler software could bypass the Agency’s Windows Installer settings, that some of the EPA’s information technology specialists believed they were exempt from the policy, and that other EPA employees and contractors installed the software without authorization. Furthermore, we discovered inconsistencies in how quickly the regional offices acted to remove the juggler software after it was detected. The installation and use of unauthorized software on EPA computers and networks represent critical cybersecurity risks and ethics violations for the Agency.

¹ Windows Installer is a component of the Microsoft Windows operating system that manages the installation, maintenance, and removal of software.

We conducted this investigation in accordance with the *Quality Standards for Investigation* published in November 2011 by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we conduct investigations in a timely, efficient, thorough, and objective manner.

BACKGROUND: According to the Inspector General Act of 1978, as amended, 5 U.S.C. §§ 401–424, OIGs are charged with preventing and detecting fraud, waste, and abuse related to the programs and operations of their agencies. To this end, our Office of Investigations “conduct[s], supervise[s], and coordinate[s] ... investigations relating to the programs and operations” of the EPA and the U.S. Chemical Safety and Hazard Investigation Board.² As part of our oversight function as an independent office of the EPA, we conduct criminal, civil, and administrative investigations, including violations of information technology and information management policies by EPA employees and contractors that potentially endanger the EPA’s cybersecurity. We also conduct audits and evaluations of the Agency’s information management processes and information security posture. For example, the OIG Office of Audit issued EPA OIG Report No. [22-E-0028](#),³ *The EPA Lacks Documented Procedures for Detecting and Removing Unauthorized Software on the Agency’s Network*, on March 30, 2022, identifying concerns regarding the presence of unauthorized software on the EPA network. The report noted over 7,000 instances of nonbase software on its network, including foreign software and malware programs that gather user information, allow remote control of the EPA user’s computer, and have a history of being used for targeted attacks.⁴ Furthermore, the report noted concerns that the Agency lacked documented software management procedures and targeted training for detecting and removing unapproved software on the EPA network.

According to the Agency’s response to EPA OIG Report No. 22-E-0028, which is included in Appendix E of the published report, the EPA implemented two corrective actions to address the concerns outlined in the report. Notably, on December 20, 2022, the EPA implemented Directive No: [CIO 2104.3](#), *Software Management and Piracy Policy*, which outlines how software should be obtained. It does not specify steps for removing unauthorized software.

The EPA’s information security and information management policies incorporate federal statutes, orders, and standards. For example, on April 10, 2024, in compliance with Office of Management and Budget Circular A-130,⁵ the EPA established Directive No: [CIO 2150-S-21.2](#), *Information Security – EPA National Rules of Behavior*. The policy establishes rules of behavior for users of EPA information systems to safeguard the systems from “misuse, abuse, loss or unauthorized access.” Before being granted access to EPA information systems, users must attest to their knowledge and understanding of their

² 5 U.S.C. § 404(a)(1).

³ EPA Off. of Inspector Gen., [22-E-0028](#), *The EPA Lacks Documented Procedures for Detecting and Removing Unapproved Software on the Agency’s Network* (2022).

⁴ According to EPA OIG Report No. 22-E-0028, nonbase software is “software that is not part of the Agency’s standard installation or otherwise loaded onto workstations as part of regular business.” According to the Cybersecurity and Infrastructure Security Agency, [malware](#) is “software used to gain unauthorized access to [information technology] systems to steal data, disrupt system services, or damage [information technology] networks in any way.”

⁵ Off. of Management and Budget, Circular [A-130](#), *Managing Information as a Strategic Resource* (2016).

responsibilities under this policy. Of note, the *EPA National Rules of Behavior* states that users must not “[i]nstall and/or download unauthorized software on an EPA computing resource without written approval by the Office of Information Management (OIM) and IRM [Information Resources Management] Branch Chief (IRMBC).” Furthermore, the policy states, “Unauthorized use of a user account or a computing resource can result in criminal penalties under Section 1030, Title 18, of the United States Code.” This statute, known as the Computer Fraud and Abuse Act, prohibits unauthorized access to government systems, including installing or using unauthorized software. Violations may result in criminal charges, fines, and imprisonment.

The EPA’s *Software Management and Piracy Policy*, which was issued two years before the *EPA National Rules of Behavior*, complies with Executive Order 13103.⁶ This policy requires that all software installed on its computers and systems be appropriately licensed, approved for use, and not pirated, specifically stating that:

- “Only software that has been approved by the IMO [information management officer] or the Agency’s OMS-EI [Office of Mission Support–Environmental Information] Office of Information Technology Operations Director and properly acquired by the Agency may be installed on EPA computer systems.”
- “Installed software, which is discovered to be unlicensed, unauthorized, obsolete, or does not comply with Agency or other standards shall be promptly uninstalled/removed.”

The EPA’s *Software Management and Piracy Policy* clarifies that violations of the policy will be dealt with under the Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. part 2635, and EPA Order 3120.1, *Conduct and Discipline*.

CONCERNS IDENTIFIED: In December 2024 and February 2025, two EPA regional offices notified us that unauthorized software, specifically juggler software, was being downloaded, installed, and used by some employees and contractors. Although mouse jigglers can have legitimate uses, the EPA has not authorized any juggler software for any use on its computers or systems, not even for use by information technology specialists. After becoming aware that this unauthorized software was being used, the Information Management Branches in Regions 5 and 8 conducted network scans. These scans uncovered that more than 120 EPA contractors and employees, including supervisors, were using juggler software. Some of these contractors and employees were information technology specialists who incorrectly believed they were exempt from Agency policy and installed juggler software to perform maintenance and repair work. Other contractors and employees installed the software for other purposes, such as to complete updates or backups that take hours. Some even placed juggler software on shared Agency drives for their colleagues to access.

⁶ Exec. Order No. 13103, Computer Software Piracy (Sep. 30, 1998).

Installing and using jigglers directly violates the *EPA National Rules of Behavior* and the EPA's *Software Management and Piracy Policy*, which all EPA employees have access to and should be familiar with. In addition, all Agency employees and contractors must annually complete Information Security and Privacy Awareness training. Although this training does not specifically address the *Software Management and Piracy Policy*, it does require each employee to open the *EPA National Rules of Behavior* and attest that they have reviewed and understand those rules. The EPA also has other procedures for detecting and removing unapproved software from its computers and systems, which the Agency developed in response to a previous OIG evaluation. None of the Agency's trainings, policies, or procedures provide any exemptions regarding the installation and use of unauthorized software for any level, role, or function of EPA employee or contractor.

The installation of unauthorized jigglers raises numerous information management and cybersecurity concerns. Although the Agency has configured Windows Installer to block the installation of unauthorized software, [REDACTED].

[REDACTED], the Agency's Windows Installer settings did not detect that EPA employees and contractors were downloading and installing the software. This vulnerability represents a larger, significant risk to the Agency's cybersecurity. [REDACTED].

In addition, recent advances in malware development make it extremely difficult for scanning tools, [REDACTED] to detect the presence of the malware. Such advances include fileless malware, which operates entirely in memory; steganography, which hides malicious code in otherwise clean files; and living-off-the-land tactics, which spread malicious code using legitimate system tools. [REDACTED].

The United States has faced recent malware attacks

Notable examples of cybercriminals and foreign intelligence services using malware against the United States' government, citizens, businesses, and organizations include the:

- Remote access trojan [attacks](#) beginning in 2021 that are perpetrated by the Chinese-based Volt Typhoon against U.S. critical infrastructure organizations.
- PlugX Malware [attacks](#) from 2014 through 2025 that were perpetrated by the Chinese-backed Mustang Panda against U.S. citizens.
- SolarWinds Supply Chain [attack](#) of 2020 that was perpetrated by Russia against U.S. citizens and government agencies.
- WannaCry Ransomware [attacks](#) in 2017 that were perpetrated by North Korean-sponsored Lazarus Group against U.S. businesses and others.
- Office of Personnel Management [breach](#) of 2015 that was perpetrated by China.

The use of unauthorized jigglers software also presents numerous ethics and cybersecurity concerns. Employees may use jigglers software to defraud workplace monitoring efforts; in other words, by using this software, employees can appear to be in active status to give the impression of working. Although our investigation did not uncover this type of misconduct, it is a risk with jigglers software. Also, because the purpose of jigglers software is to keep the computer unlocked, unauthorized individuals could more easily gain access to an employee's computer and, in turn, to the EPA's networks. As a result, personally identifiable information or classified business information stored on the EPA's networks may be potentially exposed.

We also noted inconsistencies in how Regions 5 and 8 sought to correct the installation and use of unauthorized software. Region 5 directed staff to remove the software, consistent with the *EPA National Rules of Behavior* and the EPA's *Software Management and Piracy Policy*. Despite this directive, some Region 5 staff attempted to justify why they needed the software, while some even ignored the directive. However, Region 5 did not provide any exceptions and removed all the unauthorized jigglers software that it detected. Region 5 is also undertaking disciplinary action, such as letters of counseling and suspensions, against the employees and contractors who downloaded, installed, and used the unauthorized software. On the other hand, Region 8 provided exceptions for some employees to have the software, and it is unknown whether the region is pursuing disciplinary action against those who violated the *EPA National Rules of Behavior* and the *Software Management and Piracy Policy*.

[REDACTED]

MEASURES FOR IMPROVEMENT: We are notifying the Agency of our concerns so that it may consider:

- Immediately initiating a global network scan to identify and remove jigglers and other unauthorized software.
- Identifying and implementing tools that prevent EPA employees and contractors from downloading, installing, and using jigglers and other unauthorized software, [REDACTED].
- Conducting routine global network scans, including of shared servers, devices, and cloud storage, and removing any unauthorized software that is identified.
- Ensuring nationwide Agency consistency in how EPA regions identify and remove unauthorized software, as well as disciplinary actions for violations.

~~CUI//PRIVILEGE~~

- Ensuring that the EPA's procedures for detecting and removing unapproved software from its computers and systems remain up-to-date and accessible, and providing reoccurring training on these procedures.⁷

Until the above actions can be implemented, the EPA should continue to provide its annual training encompassing the *EPA National Rules of Behavior*, send emails to all EPA employees and contractors reminding them of the requirement to comply with the *EPA National Rules of Behavior* and the *Software Management and Piracy Policy*, and educate all employees and contractors about the penalties associated with violating these policies.

We are notifying the Agency of our concerns so that it may take the steps it deems appropriate and necessary to correct the identified vulnerabilities. If the EPA decides it is appropriate to take, or plan to take, action to address these vulnerabilities, we would appreciate notification of that action. Should there be any questions regarding this report, please contact Acting Assistant Special Agent in Charge [REDACTED] at [REDACTED] or [REDACTED] or me at [REDACTED] or [REDACTED].

cc: Nicole N. Murley, Acting Inspector General

Tiffany McNeill, Director, Office of Information Technology Operations, Office of Mission Support

Tonya Manning, Chief Information Security Officer, Office of Mission Support

Paige Hallen Hanson, Chief Financial Officer, Office of the Chief Financial Officer

Anne Vogel, Regional Administrator, EPA Region 5

Cyrus Western, Regional Administrator, EPA Region 8

⁷ EPA Off. of Inspector Gen., [22-E-0028](#), The EPA Lacks Documented Procedures for Detecting and Removing Unapproved Software on the Agency's Network (2022).



Whistleblower Protection

U.S. Environmental Protection Agency

The whistleblower protection coordinator's role is to educate Agency employees about prohibitions against retaliation for protected disclosures and the rights and remedies against retaliation. For more information, please visit the OIG's whistleblower protection [webpage](#).

Contact us:



Congressional & Media Inquiries: OIG.PublicAffairs@epa.gov



EPA OIG Hotline: OIG.Hotline@epa.gov



Web: epaoig.gov

Follow us:



X: [@epaoig](https://twitter.com/epaoig)



LinkedIn: linkedin.com/company/epa-oig



YouTube: youtube.com/epaoig



Instagram: [@epa.ig.on.ig](https://www.instagram.com/epa.ig.on.ig)



www.epaoig.gov