




EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

October 8, 2021

M-22-01

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director 

SUBJECT: Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response

Executive Order 14028 (EO), *Improving the Nation's Cybersecurity*,¹ directs the Federal Government to adopt a robust Endpoint Detection and Response (EDR) solution as part of the shift in cyber defense from a reactive to a proactive posture. EDR will improve the Federal Government's ability to detect and respond to increasingly sophisticated threat activity on Federal networks. This memorandum provides implementation guidance to agencies² as they accelerate the adoption of EDR solutions and work to improve visibility into and detection of cybersecurity vulnerabilities and threats to the Government, as defined in EO 14028. Through a collective effort, the Federal Government will achieve:

- Improved agency capabilities for early detection, response, and remediation of cybersecurity incidents on their networks, using advanced technologies and leading practices.
- Agency enterprise-level visibility across components/bureaus/sub-agencies to better detect and understand threat activity.
- Government-wide visibility through a centrally located EDR initiative, implemented by the Cybersecurity and Infrastructure Security Agency (CISA), to support host-level visibility, attribution, and response across Federal information systems.

Endpoint Detection and Response

EDR combines real-time continuous monitoring and collection of endpoint data (for example, networked computing devices such as workstations, mobile phones, servers) with rules-based automated response and analysis capabilities. Compared to traditional security solutions,

¹ Executive Order 14028, *Improving the Nation's Cybersecurity* (May 17, 2021), available at <https://www.federalregister.gov/d/2021-10460>.

² As used in this memorandum, "agency" generally has the meaning given in 44 U.S.C. § 3502, but does not refer to the Department of Defense or agencies in the Intelligence Community.

EDR provides the increased visibility necessary to respond to advanced forms of cybersecurity threats, such as polymorphic malware, advanced persistent threats (APTs), and phishing. Moreover, EDR is an essential component for transitioning to zero trust architecture, because every device that connects to a network is a potential attack vector for cyber threats.

Advancing EDR Government-wide

As the Federal Government continues to adopt an enterprise approach for cyber defense, it is vital that agencies collaborate in the development and deployment of EDR solutions to promote best-practice sharing and drive operational efficiency. To further the goal of centrally managing the information needed to support host-level visibility, attribution, and response with respect to agency information systems:

- Within 90 days, agencies should provide CISA access to current enterprise EDR deployments or engage with CISA to identify future state options.
- Within 90 days, CISA shall develop a process for continuous performance monitoring to help agencies ensure that EDR solutions are deployed and operate in a manner that will detect and respond to common threats.
- Within 90 days, CISA, in coordination with the Chief Information Officer (CIO) Council, shall provide recommendations to OMB on ways to further accelerate Government-wide EDR efforts.
- Within 90 days, CISA, in coordination with the CIO Council, shall develop and publish a technical reference architecture and maturity model for agency consumption.
- Within 180 days, CISA, in coordination with the CIO Council, shall develop a playbook of best practices for EDR solution deployments to achieve Government-wide operational visibility.

Agency EDR Implementation Responsibilities

As agencies work to deploy and mature their EDR solutions, they shall:

- Within 120 days, conduct an analysis, in coordination with CISA, to assess the current status of their EDR capabilities by identifying any gaps in existing EDR deployments.
- Coordinate with CISA for current and future EDR solution deployments to confirm that the solution aligns with CISA's technical reference architecture and appropriate data is gathered from the widest number of endpoints.
- As discussed in the section above, provide CISA with access to their current and future EDR solutions to enable proactive threat hunting activities and a coordinated response to advanced threats, and to facilitate, as appropriate, network access to CISA personnel and contractors supporting implementation of the EDR initiative.
- Ensure that EDR solutions are appropriately resourced and staffed by working with their Chief Financial Officer and OMB Resource Management Office to confirm that sufficient funding is programmed to maintain the EDR tool through its lifespan and account for any potential updates or licensing requirements.

- Ensure that endpoint data is consolidated, retained, and archived in a manner that supports analysis and insight, to be defined in the technical reference architecture developed by CISA.
- Ensure that EDR solutions are consistent with applicable privacy and statistical laws and policy.

Policy Assistance

All questions or inquiries should be addressed to the OMB Office of the Federal Chief Information Officer (OFCIO) via email: ofcio@omb.eop.gov.