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

THE DIRECTOR

May 22, 2026

M-26-14

MEMORANDUM TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought
Director

SUBJECT: Ensuring Effective and Efficient Agency Logging and Network Visibility to Defend Against Evolving Cyber Threats

As recognized by President Trump's Management Agenda,[1] agencies[2] must "defend against and persistently combat cyber enemies," who continue to evolve in scale, speed, and sophistication. Threat actors have increasingly used automation and artificial intelligence to accelerate attacks against critical systems. These enhanced capabilities can help threat actors rapidly gain unauthorized access to a system, move from that system to others, and maintain their illicit access undetected over a substantial period of time. To mitigate the risk posed by these intensifying digital threats, agencies need the ability to rapidly detect, respond to, and analyze anomalous activity on their networks. Key to that ability is appropriate event logging—the timely and consistent recording of significant activities that take place in an information system. Agencies rely on information from logs to understand activity across their systems, recognize events that require attention, and support the analysis and response actions that protect sensitive data and maintain operations.

In 2021, OMB issued Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, to raise logging baselines and enhance agencies' knowledge of events occurring in their systems. Implementation of that memorandum improved foundational capabilities across agencies. However, some requirements, such as the retention of vast quantities of logging data without clear utility, proved neither operationally feasible nor cost-effective for most agencies. To address these inefficiencies and the evolving cyber threat environment, this memorandum directs agencies to employ a risk-based, prioritized logging approach.

---

[1] Available at https://www.whitehouse.gov/wp-content/uploads/2025/12/M-26-03-Presidents-Management-Agenda.pdf.

[2] For the purposes of this memorandum, "agency" has the meaning given in 44 U.S.C. § 3502. The requirements established by this memorandum do not apply to national security systems, as defined in 44 U.S.C. § 3552(b)(6), or to systems of the Department of Defense or Intelligence Community that are described in 44 U.S.C. § 3553(e).

Effective immediately, OMB Memorandum M-21-31 is rescinded. Going forward, as described below, agencies shall work within an adaptive framework that enables them to effectively and efficiently monitor their networks while minimizing red tape and containing costs.

Prioritization

In organizing and resourcing their logging activities, agencies must prioritize two objectives:

1. Continuous Event Monitoring (CEM)

Logs, log management, and logging infrastructure that enable agencies to monitor network activity in real time, promptly flag anomalous activity, and respond to that activity in a timely manner. These logs are typically ingested and monitored by a Security Operations Center (SOC).

2. Threat Hunting, Investigation, Response, and Forensics (THIRF)

Logs, log management, and logging infrastructure that enable agencies to investigate and perform forensic analysis of network activity after a known or suspected compromise with the purpose of mitigating, remediating, and recovering from threat actor activity. To enable THIRF, agencies must maintain sufficient hot and cold storage as well as the capability to retrieve and centralize logging data from multiple sources to map attack patterns.

Each agency must pursue these objectives with respect to all information systems owned or operated by the agency or by third parties on the agency's behalf, including any Internet of Things (IoT) devices or operational technology (OT) that is part of or constitutes such an information system.[3]

Reference Architecture

Within 90 days of the date of this memorandum, the Cybersecurity and Infrastructure Security Agency (CISA), in coordination with OMB and the Chief Information Security Officer (CISO) Council, will develop a logging reference architecture (LRA) that satisfies the requirements in this memorandum and assists agencies in meeting CEM and THIRF objectives. The LRA will serve as a core source of guidance for agencies on how to implement their CEM and THIRF logging capabilities, allowing them to build upon their progress under M-21-31 while affording them greater flexibility to accommodate their disparate mission requirements and associated cybersecurity risks. Agencies must adhere to the reference architecture by the timelines outlined in the "agency actions" section of this memorandum. The LRA will be published at https://www.cisa.gov/Logging.

[3] For the purposes of this memorandum, "information system" has the meaning given in 44 U.S.C. § 3502(8).

Agency Logging Plan

Agencies must submit an Agency Logging Plan to OMB and CISA within 90 days of the publication of the LRA. This plan must describe the operational steps required for the agency to deploy and maintain effective CEM and THIRF objectives. The plan will document the series of actions that will be taken to achieve the minimum baseline requirements defined in this memorandum as well as any additional log collection and activities that will be conducted to achieve CEM and THIRF objectives, with consideration given to the agency's threat environment, risk profile, and mission as provided in the guidance of the CISA Logging Reference Architecture. Each agency should periodically update its plan as necessary.

Measuring Maturity

This memorandum establishes a revised maturity model (Appendix C) to guide and measure agency implementation of logging requirements. The maturity model defines a set of performance benchmarks that correspond to varying levels of proficiency and sophistication in the following functions: visibility into system inventory, log management planning, log collection, and data retention. Agencies will measure and report on progress in terms of the percentage of systems that are determined to be operating at each maturity level.

Log Access Requirements

In the event of a known or suspected compromise of one or more Federal networks, agencies shall provide logs and other relevant data to CISA and the Federal Bureau of Investigation (FBI) upon request, to the extent consistent with applicable law, to assist in incident response, investigation, and remediation. Agencies shall provide such data in a format and by means agreed upon by the agency and CISA or the FBI as appropriate. To the greatest extent practicable, agencies shall provide access to logs within the timeframes requested by CISA or the FBI.

In cases in which agency data is subject to relevant statutory, regulatory, or judicial access restrictions, the Directors of CISA and the FBI will comply with any processes and procedures required to access such data or work with the agency to develop an appropriate administrative accommodation consistent with any such restrictions, if such an accommodation is legally available.

Agency Actions

CISA, in coordination with OMB and the CISO Council, will:

1) Publish the LRA within 90 days of the date of this memorandum;
2) Notify agencies within five business days of any published updates to the LRA; and
3) Provide logging implementation technical support and advice to agencies through channels such as frequently asked questions (FAQs), interagency engagements (e.g., workshops, focus groups, communities of practice), training, or direct support opportunities, as appropriate.

All Agencies must:

Within 90 days of the release of the LRA	Complete the first version of the Agency Logging Plan, providing for fulfillment of this memorandum's minimum requirements and using the guidance and resources within the Logging Reference Architecture.
Within 120 days of the release of the LRA	Achieve a minimum of Basic (Level 1) across all elements of the maturity model.
Within 180 days of the release of the LRA	Achieve a minimum of Intermediate (Level 2) across all elements of the maturity model.
Within 320 days of the release of the LRA	Achieve a minimum of Advanced (Level 3) across all elements of the maturity model.
Ongoing Actions: After CISA notifies agencies that there is an updated version of the logging reference architecture:	• Within 30 calendar days, update the Agency Logging Plan. • Within 60 calendar days, achieve a minimum of "Intermediate" across all elements of the maturity model. • Within 120 calendar days, achieve a minimum of "Advanced" across all elements of the maturity model.

Policy Assistance

All questions or inquiries concerning this memorandum should be addressed to the OMB Office of the Federal Chief Information Officer at ofcio@omb.eop.gov. All questions or inquiries concerning the LRA should be addressed to CISA through resources available at https://www.cisa.gov/Logging.

Appendix A: Base Requirements for the Logging Reference Architecture

The Logging Reference Architecture will address the following topics and meet the following requirements:

Prioritization	The logging reference architecture (LRA) will provide prioritization guidance for achieving continuous event monitoring (CEM) and threat-hunting, investigation, response, and forensics (THIRF), with an emphasis on High Value Assets[4] and High Impact Systems.[5] This guidance will enable agencies to determine which course to follow to best achieve their CEM and THIRF capabilities based on agency mission.
Alignment with zero trust	CISA's Zero Trust Maturity Model defines the *Visibility and Analytics* cross-cutting capability that supports and enables all five Zero Trust pillars. Zero Trust also assists Federal agencies in making risk-based decisions for implementations in support of CEM and THIRF. The LRA will align with the Zero Trust Maturity Model.
Log Centralization	The LRA will offer options for building CEM and THIRF capabilities through either a centralized access deployment or centralized architecture deployment (or a hybrid of both). Centralization and/or centralized access and visibility will occur at the highest-level security operations center (SOC) of each agency.
Log Collection Containing Risk of Incidental Sensitive Data Exposure	The LRA will include guidance to ensure that logs will not capture or expose data in contravention of law. It will also advise agencies on how to protect the confidentiality and integrity of sensitive log data.
Internet of Things (IoT) and Operational Technology (OT)	The LRA will provide guidance on implementing logging capabilities for agency IoT and OT, including IoT devices and OT that do not have native logging capability.
Artificial Intelligence (AI)	The LRA will discuss methods of using AI technologies for enhancing CEM and THIRF capabilities. This discussion will reference applicable governmentwide AI policy and guidance.
Self-Assessment	The LRA will explain how agencies may conduct self-assessments on their CEM and THIRF capabilities, as well as their logging maturity.
Data Retention Guidance	The LRA will offer recommendations on data retention practices that exceed the minimum requirements described in this memorandum.
Updates	The LRA will be re-evaluated at least once a year for necessary updates, enhancements, and adjustments to account for emerging technologies and changes in threat landscape, frameworks, strategies, and opportunities.

[4] OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf, explains how agencies are to identify high value assets.

[5] An information system for which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of "high" pursuant to the National Institute of Standards and Technology's Federal Information Processing Standard (FIPS) 199.

Appendix B: Minimum Logging Baseline Requirements and Objectives

1. Retained logs must be actively searchable[6] for a minimum of 6 months after creation to support continuous event monitoring (CEM). They must be retrievable[7] for a year after creation to support threat-hunting, investigation, response, and forensics (THIRF). (Note that meeting these minimum retention requirements for cybersecurity purposes does not relieve agencies of the obligation to comply with other applicable requirements, such as those established by agency-specific or government-wide records schedules.)

2. Log storage may be decentralized; however, logs must be readily available to the top-level agency security operations center (SOC) to achieve CEM and THIRF objectives. Agencies are encouraged to evaluate one or more approaches to achieve this objective and to seek any guidance available in the LRA. Agencies may consider collecting logs in enterprise security information and event management software or equivalent, forwarding logs to a central location, setting appropriate access authorizations across distributed logs, or taking a hybrid approach that combines centralized storage with federated access.

3. Logs must include a consistently accurate timestamp. To ensure accuracy, network time must be synchronized to a traceable time source designated within the agency. To ensure accuracy, network time must be synchronized to Network Time Protocol (NTP) or equivalent mechanisms to a traceable time source designated within the agency. Agencies are encouraged to use authoritative time sources traceable to the U.S. Naval Observatory or the National Institute of Standards (NIST), where feasible.

4. Agencies should use tools and resources such as Continuous Diagnostics and Mitigation (CDM), Hardware Asset Management (HWAM), and Software Asset Management (SWAM) data to determine whether log coverage encompasses all information technology in agency information systems, including internet-of-things (IoT) devices and operational technology (OT).

5. At a minimum, agencies must collect logs that support the following activities in furtherance of the CEM and THIRF objectives:

    a. Determining the identity used for performing operations in applications and on systems.
    b. Determining source and destination network address information, including protocols, ports, and session attributes.
    c. Identifying object/resource/data events for accessed, modified, or destroyed items.
    d. Identifying actions that affect changes to privilege levels.

---

[6] In this context, “searchable” means that the data can be immediately used for cyber defense. Detections and analytics can be applied to the data without requiring additional steps related to preparation of the data.
[7] As used here, “retrievable” means that the data can be used for cyber defense activities after one or more intermediary steps to prepare the data. Data preparation can consist of any actions that may be required to replay data from long-term storage in an analytics tool, such as moving the data from an archive into real-time analysis platforms, or “thawing” data in cold storage for access in a faster storage tier.

e. Identifying changes to IT/OT/IoT infrastructure (add/remove/modify endpoints).
f. Monitoring for suspicious activity identified by security tooling (e.g., intrusion detection systems, endpoint protection platforms, security gateways, etc.).
g. Monitoring, detecting, and hunting for known indicators of compromise.
h. Monitoring, detecting, and hunting for anomalous system or user activity.
i. Determining the quantity and types of data affected during an incident.
j. Determining the attack vector(s) of a cybersecurity attack, including any associated with initial access as well as lateral movement.
k. Generating appropriate automated alerts for all of the above.

Appendix C: Logging Maturity Model for an Information System[8]

Element	Ineffective (Level 0)	Initial (Level 1)	Intermediate (Level 2)	Advanced (Level 3)	Optimal (Level 4)
Inventory Visibility	The Level 1 requirements for this area are not met.	A minimum of 70% of IT/OT/IoT assets associated with the system are captured in a centralized HWAM/SWAM inventory.	A minimum of 80% of IT/OT/IoT assets associated with the system are captured in a centralized HWAM/SWAM inventory, and the data is updated daily.	A minimum of 90% of IT/OT/IoT assets associated with the system are captured in a centralized HWAM/SWAM inventory, and the data is updated daily.	A minimum of 95% of IT/OT/IoT assets associated with the system are captured in a centralized HWAM/SWAM inventory, and the data is updated daily.
Collection Coverage	The Level 1 requirements for this area are not met.	The system logs required by the Agency Logging Plan are searchable and retrievable for at least 50% of the HW/SW assets in the system inventory. Log aggregation occurs in a timely manner.	The system logs required by the Agency Logging Plan are searchable and retrievable for at least 80% of the HW/SW assets in the system inventory. Log aggregation occurs in a timely manner.	The system logs required by the Agency Logging Plan are searchable and retrievable for at least 90% of the HW/SW assets in the system inventory. Log aggregation occurs in a timely manner.	The system logs required by the Agency Logging Plan are searchable and retrievable for at least 95% of the HW/SW assets in the system inventory. Log aggregation occurs in a timely manner.
Collection Operations	The Level 1 requirements for this area are not met.	Logs generate actionable alerts covering <50% of minimum baseline logging requirements. Alerts are referenced in investigations on an ad hoc basis.	Logs generate actionable alerts covering 50–70% of minimum baseline logging requirements, and detections are periodically evaluated and tuned to enable CEM/THIRF outcomes.	Logs generate actionable alerts covering at least ≥70% of baseline logging requirements, and detections are routinely evaluated and tuned.	Logs generate actionable alerts, covering at least 95% of baseline logging requirements, and detections are routinely evaluated and tuned using advanced techniques such as machine learning or artificial intelligence.
Data Retention	The Level 1 requirements for this area are not met.	Logs are retained and retrievable for a minimum of 6 months.	Logs are retained and retrievable for a minimum of 12 months.	Logs are retained and searchable for a minimum of 3 months and are retrievable for a minimum of 12 months.	Logs are retained and searchable for a minimum of 6 months and are retrievable for a minimum of 12 months.
Log Management	The Level 1 requirements for this area are not met.	Logs are stored.	Logs are stored and encrypted at rest.	Logs are encrypted in transit and at rest, and regularly hashed for veracity.	Logs are encrypted, access is granted just in time, permissions and workloads are regularly monitored and reviewed, and logs that are retired are managed appropriately through two-gate approvals.

[8] Overall maturity is calculated based on the lowest watermark for each component in the maturity model.