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

August 10, 2021

M-21-30

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Protecting Critical Software Through Enhanced Security Measures

Background

The United States faces increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and, ultimately, the American people's security and privacy. The Federal Government must improve its efforts to detect, identify, deter, protect against, and respond to these campaigns and their perpetrators. This includes partnering with the private sector to ensure that products continuously evolve to secure against a dynamic threat environment.

The Federal Government's ability to perform its critical functions depends upon the security of its software. Much of that software is commercially developed through an often-opaque process that may lack sufficient controls to prevent the creation and exploitation of significant application security vulnerabilities. As a result, there is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely in the manner intended. The Federal Government must identify and implement practices that enhance the security of the software supply chain and protect the use of software in agencies' operational environments.

Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (May 12, 2021)[1], recognizes the importance to the Federal Government of software security – and in particular, the security of "critical software," as defined by the National Institute of Standards and Technology (NIST). The EO directs NIST to issue guidance on security measures for critical software, and further directs the Office of Management and Budget (OMB) to require agencies to comply with that guidance. The guidance from NIST, issued on July 8, 2021,[2] outlines core security measures, the implementation of which is crucial for the protection of critical software.

[1] Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[2] Available at: https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use-2

This memorandum provides instructions for the implementation of those fundamental measures required to secure the use of software falling within the definition below and directs executive departments and agencies (hereafter referred to as agencies) to implement those measures in phases. Agencies should keep in mind that the measures identified in the guidance from NIST are not comprehensive; their adoption may not eliminate the need to implement additional security measures to satisfy requirements and objectives that lie outside the scope of the NIST guidance.

I. Critical Software Definition and Required Security Measures

For the purposes of EO 14028, NIST has defined critical software as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:

- is designed to run with elevated privilege or manage privileges;
- has direct or privileged access to networking or computing resources;
- is designed to control access to data or operational technology;
- performs a function critical to trust; or
- operates outside of normal trust boundaries with privileged access.[3]

The definition applies to software of all forms (e.g., standalone software, software integral to specific devices or hardware components, cloud-based software) that is purchased for, or deployed in, information systems and used for operational purposes.

II. Implementation of Critical Software Guidance

A. Initial Phase

Government-wide implementation of NIST's guidance for the use of critical software will occur through a phased approach. During the initial implementation phase, agencies should focus on standalone, on-premise software that performs security-critical functions or poses similar significant potential for harm if compromised. Such software includes applications that provide the following categories of services:

- identity, credential, and access management (ICAM);
- operating systems, hypervisors, container environments;
- web browsers;
- endpoint security;
- network control;
- network protection;
- network monitoring and configuration;
- operational monitoring and analysis;

[3] *Definition of Critical Software under Executive Order (EO) 14028* (June 25, 2021), *available at* https://www.nist.gov/system/files/documents/2021/06/25/EO%20Critical%20FINAL_1.pdf.

- remote scanning;
- remote access and configuration management; and
- backup/recovery and remote storage.

B. Subsequent Phases

Agencies must review this guidance and ensure it is implemented across all categories of critical software described in section II.A. Subsequent phases of implementation will address additional categories of software, as determined by the Cybersecurity and Infrastructure Security Agency (CISA). The following categories of software, among others, will be included in those future phases:

- software that controls access to data;
- cloud-based and hybrid software;
- software development tools, such as code repository systems, testing software, integration software, packaging software, and deployment software;
- software components in boot-level firmware; and
- software components in operational technology (OT).

III. Government-Wide Actions and Responsibilities for Critical Software Use

To implement NIST's guidance, agencies must identify their critical software and adopt the required security measures for the use of that software. Doing so will permit the achievement of these fundamental objectives:

- Protecting critical software and critical software platforms from unauthorized access and usage.
- Protecting the confidentiality, integrity, and availability of data used by critical software and critical software platforms.
- Identifying and maintaining critical software platforms and the software deployed to those platforms to protect the critical software from exploitation.
- Quickly detecting, responding to, and recovering from threats and incidents involving critical software and critical software platforms.
- Strengthening the understanding and performance of human actions that foster the security of critical software and critical software platforms.

The following applies to all agencies:

- Within 60 calendar days of the publication of this memorandum, agencies must identify all agency critical software, in use or in the process of acquisition.
- Within one year of the publication of this memorandum, agencies must implement the security measures designated by NIST for all categories of critical software included in the initial phase.

- Agencies must incorporate security measures within one year of the publication of each guidance update from NIST, which will launch each subsequent phase of implementation.

V. NIST Actions and Responsibilities

NIST will publish updates to the definition of critical software, and associated security measures guidance, as necessary.

VI. CISA Actions and Responsibilities

CISA will maintain a list of software categories that meet the definition of critical software. CISA will also identify the categories of critical software to be included in each phase of the implementation of NIST's guidance.

VII. 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.

This table summarizes all actions in the memorandum above:

Requirement	Deadline	Responsible Body
1. Identify All Agency Critical Software, in Use or in the Acquisition Process	60 Days	All Agencies
2. Incorporate Security Measures for Specified Categories of Critical Software	1 Year	All Agencies
3. Incorporate Security Measures for Additional Software Categories Identified for Each Subsequent Phase	1 Year	All Agencies
4. Publish Updates to the Definition of Critical Software and Guidance for Security Measures	As necessary	NIST
5. Issue List of Software Categories to Be Included in Next Phase of Implementation	As necessary	CISA