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

THE DIRECTOR

February 27, 2023

M-23-13

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young

SUBJECT: "No TikTok on Government Devices" Implementation Guidance

I. Background

TikTok is a software application owned and operated by ByteDance Limited ("Bytedance"), a privately held company headquartered in Beijing, China.

The Consolidated Appropriations Act, 2023, enacted the No TikTok on Government Devices Act ("the Act"), which instructs the Director of the Office of Management and Budget, in consultation with the Administrator of General Services, the Director of the Cybersecurity and Infrastructure Security Agency, the Director of National Intelligence, and the Secretary of Defense, to develop standards and guidelines for agencies requiring the removal of TikTok from Federal information technology.[1] This memorandum fulfills that requirement by directing agencies to remove TikTok from Federal devices and providing instructions and deadlines for that removal.

II. Scope

Pursuant to the Act, this memorandum applies to "the social networking service TikTok or any successor application or service of TikTok developed or provided by ByteDance Limited or an entity owned by ByteDance Limited" ("covered application") and applies to all "executive agencies" ("agencies"), as that term is defined in 41 U.S.C § 133.[2]

This memorandum applies to all "information technology," as that term is defined in 40 U.S.C. § 11101(6) (herein after referred to as "IT"). That definition reaches not only IT owned or operated by agencies, but also IT "used by a contractor under a contract with the executive agency that requires the use" of that IT, whether expressly or "to a significant extent in the

[1] Pub. L. No. 117-328, div. R, §§ 101-02, *available at* https://www.congress.gov/bill/117th-congress/house-bill/2617.
[2] *Id.* § 102(a).

performance of a service or the furnishing of a product." That definition does not, however, "include any equipment acquired by a federal contractor incidental to a federal contract."

III. Actions

A. No later than 30 days following the issuance of this memorandum, agencies shall—

i. Identify the use or presence of a covered application on information technology;
ii. Establish an internal process to adjudicate limited exceptions, as defined by the Act and described in Section IV;
iii. Remove and disallow installations of a covered application on IT owned or operated by agencies, except in cases of approved exceptions; and,
iv. Prohibit internet traffic from IT owned by agencies to a covered application, except in cases of approved exceptions.

Agencies whose mission or operational posture prevents compliance with the timeline delineated in Section III.A. must notify the Federal Chief Information Officer prior to the deadline by sending a message to ofcio@omb.eop.gov.

B. No later than 90 days following the issuance of this memorandum, agencies shall—

i. Ensure that any new contracts issued do not contain requirements that may include the use of a covered application in the performance of the contract, except in cases of approved exceptions; and,
ii. Cease use of contracts that contain requirements that may include use of a covered application in performance of the contract or modify those contracts to conform with the prohibition on covered applications, except in cases of approved exceptions.

C. No later than 120 days following the issuance of this memorandum, agencies shall—

i. For contracts whose performance may involve use of IT by the contractor, ensure that any modification that extends the period of performance, including through exercise of an option, includes a requirement to conform with the prohibition on covered applications; and,
ii. Ensure that each agency solicitation requires conformance with the prohibition on covered applications if the solicitation meets both of the following criteria: (1) the solicitation is issued on or after the date that is 120 days after the date of this memorandum; and (2) a contract issued based on the solicitation may involve use of information technology by a contractor.

IV. Exceptions

A. Documentation

The Act permits limited exceptions to the restrictions outlined in this memorandum for law enforcement activities, national security interests and activities, and security

research.[3] Agencies should limit the use of exceptions outlined within this section to instances in which use of a covered application is critical to their mission and alternative approaches are not viable.

Exceptions must be granted by an agency head or designee of the agency head.[4] Agency heads remain responsible for ensuring that all individuals with delegated authority under this policy maintain the documentation required and take all necessary actions to mitigate risk posed by covered applications.

Blanket exceptions applying to an entire agency are not permitted. Exceptions must be exclusive to specific agency programs or operational actions covered by the exception categories below. The agency must develop and document risk mitigation actions appropriate for any use of a covered application for which an exception is granted.

Agencies must maintain documentation on each exception that includes, at a minimum, the following information:

i. Date of approval;
ii. Exception category (as outlined in part B below);
iii. Description of the circumstances under which the exception applies;
iv. Period of the exception; and,
v. Risk mitigation actions that will be taken to prevent access by a covered application to sensitive data.

Exceptions may last up to one year, after which agencies shall reevaluate them for renewal or termination. Agency heads must maintain a list of current exceptions, which must be provided to OMB upon request as described in Section V below. A copy of the documentation for any approved exception related to specific activities in a government contract must be shared with acquisition officials for inclusion, as appropriate, in relevant contract files.

B. Exception Categories

i. *National Security Interests and Activities*

An agency head may grant an exception allowing use of a covered application after first determining that such use would have a clear nexus with national security interests or activities. For example, activities performed pursuant to authorities granted under title 6, title 10, or title 50 of United States Code may have the requisite nexus, as may activities undertaken to mitigate severe damage or

[3] *Id.* § 102(b)(2)(A).
[4] This includes the authority to issue exceptions for agency operations or missions that require knowledge of such an operation or mission to remain restricted within the agency.

disruption arising in the course of a major disaster[5] or emergency[6] declared by the President.

ii. *Law Enforcement Activities*

Such activities may include those that are performed by or in coordination with an agency that is part of the Federal law enforcement community,[7] in response to a law enforcement emergency,[8] or in the course of investigating potential violations of Federal statutes or regulations.

iii. *Security Research Activities*

Such activities may include investigations to limit harm to individual, public, private, or national physical or digital infrastructure through the identification of vulnerabilities, security weaknesses, or actionable threats, as well as agency investigation into suspected malign foreign influence.

V. Reporting

Agencies shall notify OMB that they have completed all actions delineated in Section III.A no later than 90 days after the date of this memorandum. These notification documents must be signed by the agency Chief Information Officer and emailed to ofcio@omb.eop.gov.

No more than 120 days after the date of this memorandum, agencies are required to submit the number of exceptions approved to that date under each of the categories described in Section IV.B of this memorandum. Agencies shall submit that information using the CyberScope application, https://cyberscope.dhs.gov, under the tab "M-23-13 'No TikTok on Government Devices' Implementation Guidance." For questions regarding CyberScope access, please contact cyberscopehelp@cisa.dhs.gov.

A list of agency-approved exceptions and all relevant documentation under Section IV must be made available to OMB upon request.

Activities conducted under U.S.C. title 50 are exempted from the reporting requirements within this section.

VI. Other Supply Chain Concerns

If an agency determines that there is a reasonable basis to conclude that a substantial supply chain risk exists in connection with an application not covered by the Act, the agency shall submit information regarding that risk to the Federal Acquisition Security Council (FASC) consistent with 41 C.F.R. § 201-1.201.

---

[5] 42 U.S.C. § 5170.
[6] *See, e.g.*, 42 U.S.C. § 5191.
[7] 34 U.S.C. § 50102.
[8] *Id.*