Mobile Data Isolation for Complete Separation

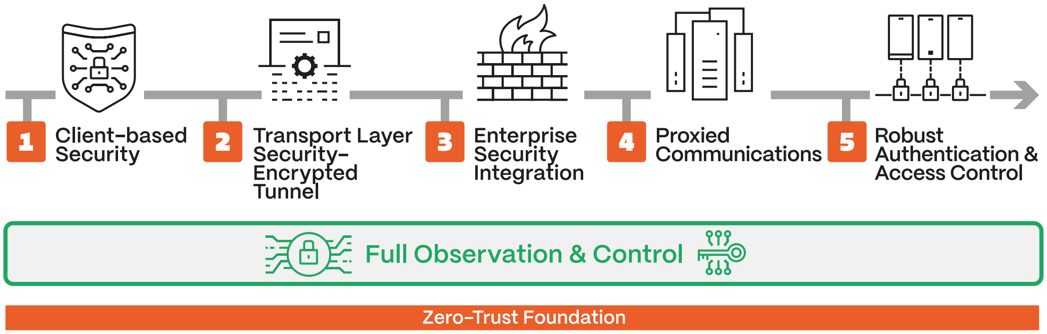
Hypori

One Device, Zero Worries™

No data access between the physical and virtual devices for compliance with the No TikTok on Government Devices Act.

This document outlines how Hypori complies with White House issued, "No TikTok on Government Devices Act," dated 27 February 2023. This memorandum mandates the removal of the TikTok social media application from the information technology systems of federal agencies, including the Department of Defense, the Intelligence Community, and the National Security Sector. It ensures that TikTok is not present on government-owned or contractor devices that interact with United States Government data.

Agencies & contractors using Hypori devices **are already in full compliance with the No TikTok on Government Devices Act.**



1 Client-based Security
2 Transport Layer Security-Encrypted Tunnel
3 Enterprise Security Integration
4 Proxied Communications
5 Robust Authentication & Access Control
Full Observation & Control
Zero-Trust Foundation

As a 100% separate, zero-trust, virtual Android OS workspace, accessible from any mobile device, Hypori transmits no data to the physical device, leaves no data at rest on your device, and keeps government data isolated and protected in the virtual device environment. It is impossible for data, malware, or aggressive data-harvesting apps on the physical device to access the Hypori environment and vice versa. Threat Systems Management Office (TSMO) described Hypori as "Virtual government-furnished equipment (GFE)", implying that the virtual instance operating within the protected network is a physically and logically separate GFE device. This virtual GFE device cannot be impacted by the mobile device, or applications operating on that edge platform. Agencies using Hypori have total control of the Hypori workspace across the application stack (Layers 1-7) with complete enterprise control of what apps are available on the virtual platform. Hypori's separate and isolated environment protects the government data and network and meets the No TikTok on Government Devices Act prescribed guidelines as detailed in this document. Implementation of Hypori does not infringe on their employees' privacy or control of personally-owned devices by restricting their downloads to their bring your own devices (BYOD). It is unnecessary to monitor users' physical devices because their personal apps can't access or infiltrate the Hypori virtual device.

Request a Demo

Addressing No TikTok on Government Devices Act

Hypori
One Device, Zero Worries™

Section III, "Actions," of the memorandum provides instructions and deadlines for the removal of TikTok on the aforementioned devices. See how Hypori addresses each action.

III. Actions

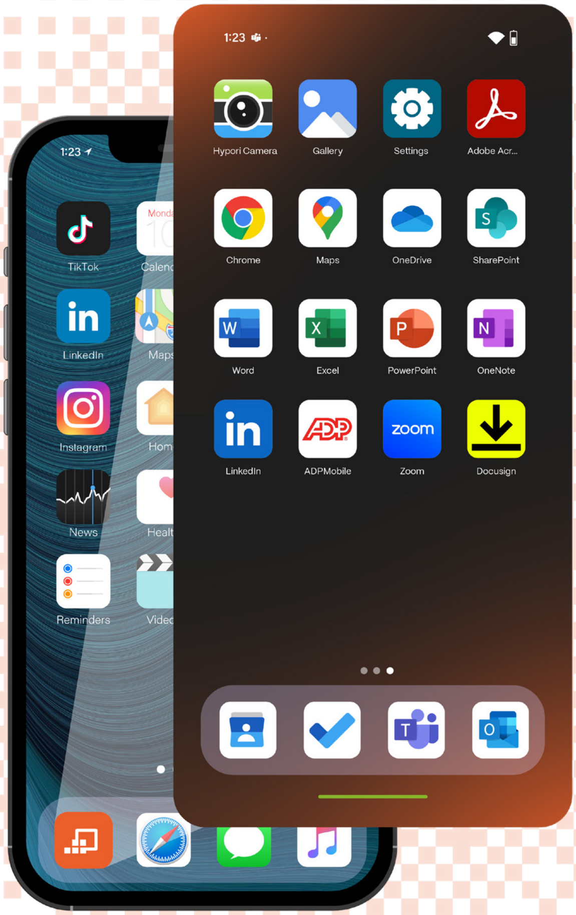
A. No later than 30 days following the issuance of this memorandum, agencies shall—

i. Identify the use or presence of a covered application on information technology;

Fully Compliant. By design, Hypori is an isolated, secure operating system that resides within the protected environment only (IL5 / NIPRNet). Access to applications within Hypori is prescribed through security templates. Users cannot independently add applications to Hypori. Complete inventory of all applications allowed and operating within is available at all times and controlled by the enterprise.

ii. Establish an internal process to adjudicate limited exceptions, as defined by the Act and described in Section IV;

Fully Compliant. Hypori and the data accessed through Hypori remain within the secured government network at all times and cannot be exposed to malicious applications on the user's mobile devices.



See it live

iii. Remove and disallow installations of a covered application on IT owned or operated by agencies, except in cases of approved exceptions; and,

Fully Compliant. This is a default feature of Hypori, as only approved apps can be loaded into the application security templates. Users do not have access to any application store, nor can they "side load" any applications. This has been tested and validated via security testing by the Army's Threat Systems Management Office (TSMO), Director of Test and Evaluation, (DOT&E), and other Defense and Intelligence Agencies.

iv. Prohibit internet traffic from IT owned by agencies to a covered application, except in cases of approved exceptions.

Fully Compliant. Hypori is set behind a security architecture that isolates all virtual workspace traffic to DOD cloud computing security requirements guide IL5 and .mil resources. Firewall rules within the architecture prevent traffic from accessing anything outside of approved sources.

For more information on Hypori's zero-trust approach to secure BYOD, please email us at info@hypori.com to request our "Hypori Defense In-Depth" whitepaper.

Why Hypori is the smarter choice

Total personal privacy

With Hypori, your organization can't see what's happening on the device, and because data is never stored locally, there's no risk of a personal device being wiped, confiscated, or subpoenaed.

Secure virtual access

Stream pixels, not data. With no data stored, processed, or transmitted on personal devices, you get secure virtual access from any mobile device with minimized risk exposure.

Worry-free BYOD

Unlike traditional MDM or application management solutions, Hypori doesn't require intrusive software that puts personal privacy at risk. Overcome user resistance and increase adoption.

Reduce risk and liability

Hypori protects your organization from costly data spillage risks and preserves your reputation while freeing up resources for growth-focused initiatives.

Proven and compliant

Hypori's zero-trust architecture meets the highest security and compliance standards. Trusted by global systems integrators, defense, government, healthcare, and other regulated industries.

Easy and convenient

Configure, deploy, and manage users and virtual devices through the Hypori Console for easy on-boarding and deployment at scale.

Request a Demo