NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

OPERATIONS SECURITY (OPSEC) ADVISORY

THIS PRODUCT WAS PUBLISHED BY NCSC'S ENTERPRISE THREAT-MITIGATION DIRECTORATE AND THE NATIONAL OPERATIONS SECURITY PROGRAM (NOP) OFFICE

TikTok Concerns and Vulnerabilities

OPSEC Advisory 2023-001

March 2023

BACKGROUND:
On 27 February 2023, the Office of Management and Budget (OMB) issued a *Memorandum for the Heads of Executive Departments and Agencies* ("agencies") with implementation guidance (link here) for the "No TikTok on Government Devices Act." This document directs organizations to:

- Remove the covered application (TikTok) from Information Technology (IT) owned or operated by agencies.
- Cease use of contracts that contain requirements for the covered application while ensuring contract solicitation and new contract language do not require use of the covered application.
- Establish processes for exceptions to policy and for reporting compliance to OMB.

OPSEC GUIDANCE:
In light of this guidance, the National OPSEC Program (NOP) Office believes some supporting information and amplifying guidance may be helpful to the OPSEC community. Below is a series of recommendations and talking points that OPSEC program officials can use when advising their stakeholder offices on implementation and workforce awareness campaigns regarding this Advisory.

The NOP strongly encourages all U.S. Government (USG) employees and affiliated staff to avoid using TikTok and other foreign-owned social media applications on personal devices. Underpinning this recommendation is the foreign access and control of user data which may create vulnerabilities or present risks for personnel and jeopardize USG information.

- Social media applications collect data on device model, screen resolution, current Operating System (OS), phone number, email address, location, keystroke patterns, and contact lists. Even if an individual does not have an active TikTok account, accessing a TikTok video link still captures information about a user and the device (e.g., model, Internet Protocol (IP) address, location, device advertising identification, etc.).
- Foreign governments could compel application owners to provide user data including those of U.S. citizens. [In TikTok's case, the parent company is ByteDance, which has reported ties to the Chinese government.]
- Many social media applications contain technical vulnerabilities that can be exploited by intelligence/security services or co-opted by hackers for nefarious purposes. [TikTok uses the

unsecure Hypertext Transfer Protocol (HTTP) for delivering videos instead of the more secure Hypertext Transfer Protocol Secure (HTTPS).]

- Even if USG personnel adhere to these recommendations, they can still be vulnerable if friends and family unwittingly reveal personal attributes and social connections. Many social media applications employ sophisticated facial recognition, geolocation tagging, and artificial intelligence capabilities which allow the platform to isolate who is in a particular video, where it was downloaded, and what keywords/topics were referenced.

- Foreign adversaries can then use this collected metadata to help identify USG employees, establish targets based on access to key collection topics (e.g., military, diplomatic, economic, research, health, etc.), and exploit personal vulnerabilities. Such intimate detail greatly enhances an adversary's ability to conduct elicitation, enable technical penetration of personal IT devices, and perhaps ultimately increase insider threat risk.

RESOURCES:
For more information, please contact the National OPSEC Program Office at NOP@dni.gov.