Department of Transformation and Shared Services
Governor Sarah Huckabee Sanders
Secretary Joseph Wood
Director Edward Armstrong

Memorandum

To: The Honorable Sarah Huckabee Sanders, Governor of Arkansas
Gretchen Conger, Chief of Staff

From: Edward R. Armstrong, Director of the Office of State Procurement
Jonathan Askins, Director of the Division of Information Systems

Date: April 6, 2023

Subject: Compliance with Executive Order 23-06

Background:

On January 10, 2023, the day of her inauguration, Governor Sanders issued Executive Order 23-06 (EO 23-06), ordering the Director of the Office of State Procurement (OSP), in consultation with the Director of the Division of Information Systems (DIS), to:

(1) Complete a review of all relevant materials, including, as appropriate, any documentation prepared or used by state and federal government agencies, cybersecurity firms, and other experts in the State of Arkansas; and make a preliminary determination as to whether any information or communications, products, or services being used by any entity subject to their oversight could pose an undue or unacceptable risk to the safety and security of the State of Arkansas on account of its connection with or use by a foreign adversary; and

(2) On or before April 10, 2023, submit a report to the Governor responding to the directive under paragraph (1) of EO 23-06.

Results of Threat Analysis:

In faithful compliance with EO 23-06, paragraphs (1) and (2), the Director of OSP, in consultation with the Director of DIS, reports:

Initial review of relevant materials confirms that the risk of China and other foreign adversaries threatening the safety and security of the State of Arkansas through the State's information systems, communications systems, procurement of technological products, and cyber services is real, not fully known, expanding, and evolving.[1] TikTok has clearly been identified as a threat to national security,[2] but is merely one of an undetermined number of applications that a

[1] *See* Annual Threat Assessment of the US Intelligence Community, ATA-2021-Unclassified-Report.pdf (dni.gov).
[2] *See* FBI director warns Senate of Chinese control over TikTok data - Roll Call; FBI chief says TikTok 'screams' of US national security concerns | Reuters (FBI Director and Other top U.S. intelligence officials including Director of National

foreign adversary could use to threaten our safety and security.[3] Because the threat is not fully known, a complete and final review of all relevant materials is impossible. Instead, the State will need to set up an ongoing process to monitor and respond to existing and emerging threats pursuant to an adaptive framework that is regularly reviewed and updated to be as responsive as reasonably possible.

Effective and comprehensive management of the risk presented by information, communications, products, or services from China or other foreign adversaries will require a multifaceted approach that involves the entire enterprise—from senior leaders/executives providing the strategic vision and top-level goals and objectives for the organization; to mid-level leaders planning, executing, and managing projects; to individuals on the front lines operating the State's information systems and supporting its various missions and public functions. Implementing a uniform and comprehensive risk management across the State and its various department and divisions will require a central, authoritative standard that governs how each of the entities that comprise it shall: (i) frame risk *(i.e*., establish the context for risk-based decisions); (ii) assess risk; (iii) respond to risk; and (iv) monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations. This exceeds the combined capabilities of OSP and DIS. However, with the Governor's executive support, DIS can develop and publish the uniform standard for framing, assessing, assessing, and responding to risks and OSP can ensure that compliance with these standards is incorporated into the terms of any information technology contracts that it awards. To be truly effective, this framework will need to extend beyond the reach of DIS and OSP and be embraced and implemented by all the various leaders entrusted with entity oversight. Because the State's information network will only ever be as strong as its weakest link, all of them will need to be tasked with the duty of working to reduce risk and committed to securing their portion of shared responsibility under the State's cyber-security risk framework.

At the invitation of the Governor, the Director of DIS has developed a proposed statewide framework for (i) assessing/remediating existing risk, in Arkansas state agencies' current installed base; (ii) assessing/monitoring technology risk on an ongoing basis. (iii) mitigating potential risk, in the IT procurement and deployment processes; and (iv) providing an education process, including quarterly briefings to the agencies' Chief Information Officers (CIOs) and Chief Security Officers (CSOs), of the ongoing security assessment/monitoring findings:

(1) The Arkansas State Cyber Security Office, in conjunction with the state agencies' CSOs, have reviewed the state's IT installed base and identified sources of potential risk, in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-37 Rev. 2, "Risk Management Framework for Information Systems and Organizations". Where said risk has been identified, mitigation measures have been taken. These measures have included the isolation and/or removal of technology deemed to present an unacceptable risk. Further measures have included detailed review of communications log data, to ensure the identified infrastructure component(s) is/are communicating only with authorized recipients.

(2) In accordance with both government and private industry best practices the Arkansas State Chief Information Security Officer (CISO), in conjunction with the other state agencies, has implemented an ongoing technology assessment process. This process derives guidance

Intelligence, CIA Director, and National Security Agency Director agreed at the hearing that TikTok posed a threat to U.S. national security).

[3] See Washington Post, How TikTok Became a US-China National Security Issue (Noting that, based on national security concerns, India banned use of TikTok and dozens of other apps developed by China in 2020).

from Federal Government information security standards and guidelines. However, the final determination relative to the application of said Federal Government guidance, and degree to which it is applied is reserved to the TSS. The referenced Federal Government guidance documents include, but are not limited to:

a. John S. McCain National Defense Authorization Act for Fiscal Year 2019 Prohibited Manufacturers List (updated in 2020);
b. U.S. Department of Commerce Bureau of Industry and Security "Entity List"; and
c. Federal Communications Commission Public Safety and Homeland Security Bureau List of Equipment and Services Covered by Section 2 Of the Secure Networks Act.

(3) DIS reviews/approves all significant state executive agency IT procurements, for technical soundness and adherence to architectural standards. As such, DIS is uniquely positioned to screen said procurements for questionable security choices. Working with our technology vendor partners, DIS will be able to identify potentially risky solutions and recommend more secure options, as appropriate.

Wherever possible and cost-effective (*e.g*. laptop and desktop computers, servers), Arkansas state agencies acquire technology in a "bare metal" state. DIS, the agencies, or the agencies' contractors will install/configure the operating system and applications software (*e.g*. Microsoft Windows, VMware, Red Hat Linux, Microsoft Office 365, etc.) locally. This practice eliminates the possibility of malicious operating system and/or application software being introduced, onto the systems, at their place of manufacture. This ensures that systems are deployed to their users, in a known, trusted state.

(4) The Director of DIS, and the State CISO meet monthly with the other state agencies' CIOs and CSOs. These meetings ensure a timely, bi-directional flow of information between DIS and the other state IT professionals. On at least a quarterly basis, or as-required, time will be set aside for the CISO to provide an update of the quarter's technology assessment process findings. This will ensure the expeditious dissemination of security-related information, across state government, thereby reducing Arkansas state government's risk profile.

OSP and DIS will continue working together, on an ongoing basis, to develop policies and contract terms that align with the above DIS plan.