

EXECUTIVE ORDER TO PROTECT STATE INFORMATION AND COMMUNICATIONS TECHNOLOGY FROM THE INFLUENCE OF THE ADVERSARIAL FOREIGN GOVERNMENTS

WHEREAS: The People’s Republic of China (“China”) is locked in economic, political, and military competition with the United States. It is a foreign adversary that presents serious challenges to our values, our security, and our economy;

WHEREAS: The challenges posed by China are particularly acute with respect to information and communications technologies. According to the Office of the Director of National Intelligence, China “presents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private sector networks”;

WHEREAS: The United States Department of Commerce has decided to review certain transactions involving Chinese persons and entities because they may pose an unacceptable risk to the national security and interests of the United States;

WHEREAS: The Arkansas Department of Transformation and Shared Services oversees both the Office of State Procurement (OSP) and the Division of Information Systems (DIS);

WHEREAS: The Director of the OSP is responsible for promulgating rules that modernize and promote quality, integrity, and public confidence in state procurement;

WHEREAS: The Director of the DIS, who also serves as Arkansas’s Chief Technology Officer, is responsible for promulgating rules related to the provision of information technology products and solutions to state entities, public primary and secondary schools, cities and counties, and public safety organizations;

WHEREAS: The information and communications systems of state entities, public primary and secondary schools, cities and counties, and public safety organizations face persistent threats that could harm Arkansans;

WHEREAS: Information and communications systems sold by vendors under the influence of China, whether through contract, investment, partnership, or other relationships, are particularly vulnerable to infiltration, exploitation, and harm through tactics such as the incorporation of malicious code or the ability to observe or extract sensitive information stored within or traveling through those systems;

WHEREAS: The video application known as TikTok, which is owned by ByteDance LTD., a Chinese company with significant ties to the Chinese Communist Party, is of particular concern;

WHEREAS: TikTok can harvest large amounts of data from devices on which it is installed, including information regarding when, where, and how users interact with the Internet;

WHEREAS: TikTok has confirmed that China-based employees can access data regarding the Internet activity of people located in the United States;

WHEREAS: The National Intelligence Law of the People's Republic of China requires all Chinese businesses to assist in China's intelligence operations, including through sharing data with the Chinese government; and

WHEREAS: It is the position of this administration to undertake strong and prudent measures to protect the information and communications systems used by state entities, public primary and secondary schools, cities and counties, and public safety organizations from harm to prevent both unauthorized access and exploitation of the critical data stored within and traveling through those systems.

NOW, THEREFORE, I, SARAH HUCKABEE SANDERS, acting under the authority vested in me as the Governor of the State of Arkansas, do hereby order the following:

1. Within sixty (60) days of the effective date of this Order, the Director of the OSP, in consultation with the Director of the DIS, shall:
 - a. 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
 - b. 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.

1. Within ninety (90) days of the effective date of this Order, the Director of the OSP, in consultation with the Director of the DIS, shall submit a report to the Governor in response to the directive under paragraph (1) of this Order.

1. The prohibition of the installation of, connection to, or use of TikTok on any state network or state-issued information or communications technology device, including all desktop computers, laptop computers, tablets, and mobile phones by any entity overseen by either the Director of the OSP or the Director of the DIS.

1. Within thirty (30) days of the effective date of this Order, the Director of the OSP, in consultation with the Director of the DIS, shall implement efficient and effective plans to uninstall, disconnect, and prevent the use of TikTok with respect to all state networks and state-issued devices described in Paragraph (3) of this Order and to prevent all future installations, connections, or uses of TikTok on such networks and devices.

1. Within thirty (30) days of the effective date of this Order, the Director of the OSP shall certify implementation of the plan described in Paragraph 4 of this Order.

1. The Governor may grant extensions for the deadline set forth herein as she may deem appropriate.

This Executive Order shall become effective upon its signing and shall remain in full force and effect until amended or rescinded by further executive orders.

IN TESTIMONY WHEREOF, I have hereunto set my hand and cause the Great Seal of the State of Arkansas to be affixed this 10th day of January, in the year of our Lord 2023.