[redacted]

Sent: Saturday, July 19, 2025 12:17 PM

[redacted]

Subject: [EXT] United States and South Dakota State Government systems exposed to CHINA

South Dakota Canvassing Group
[redacted]

July 19, 2025

Governor Larry Rhoden
Cc: Attorney General Marty Jackley
Cc: Secretary of State, Monae Johnson
Cc: Speaker of the House, Jon Hansen
Cc: Speaker Pro Tempore, Karla Lems
Cc: South Dakota Freedom Caucus
Cc: South Dakota State Legislature
Cc: Government Operations and Audit Committee

Honorable Representatives of the Republic,

I am writing to bring your attention to a matter of national security that directly affects the State of South Dakota, and the security of our cyber networks.

An explosive whistleblower report reveals that Microsoft Azure Government platforms are compromised by foreign nationals, particularly individuals located in China.
The United States Government, under the direction of then President, Barack Hussein Obama, authorized a work around with Microsoft, which allowed Microsoft to use the "global workforce", in particular Chinese nationals based in China, to provide tech support for DOD Cyber Systems on the Microsoft Government Azure platform, allowing China to have full access to Classified information out of the Pentagon. This has been happening for over 10 YEARS! https://x.com/ChanelRion/status/1945841366073798661

United States Senator Tom Cotton issued a letter to Secretary of Defense Pete Hegseth stating *"The U.S. government recognizes that China's cyber capabilities pose one of the most aggressive and dangerous threats to the United States, as evidenced by infiltration of our critical infrastructure, telecommunications networks, and supply chains. DoD must guard against all potential threats within its supply chain, including those from subcontractors."*
https://www.cotton.senate.gov/news/press-releases/chairman-cotton-to-hegseth-dod-cannot-allow-china-to-infiltrate-its-critical-infrastructure

Secretary of Defense Pete Hegseth revealed the Department of Defense had no knowledge of this agreement but has promised to take action to remove Chinese nationals from accessing United States Department of Defense and government IT platforms.
https://x.com/SecDef/status/1946324468898426899

In 2017, President Barack Hussein Obama's head of the Department of Homeland Security, Jeh Johnson, designated the federal election infrastructure as critical national infrastructure, which requires all election infrastructure to meet FEDRAMP and FISMA security standards. Currently, none of our state elections systems meet these requirements.
https://www.dhs.gov/archive/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

The South Dakota Secretary of State has contracted with KNOWiNK (formerly Bpro, Inc of Ft. Pierre, SD) for the Total Vote voter roll maintenance and election night reporting system. This centralized, federalized, internet connected, cloud hosted program resides on the Microsoft Azure Government platform. Here is the contract for South Dakota Secretary of State with Microsoft Azure. https://open.sd.gov/contracts/31/24-3100-003.pdf

All personal identifying information of every registered voter in the state of South Dakota, along with all electronic election night reporting data and results has potentially been exposed or accessed by foreign nationals. This is a violation of national security, and it must be addressed immediately.

The Microsoft Azure Government program has been found to be compromised by China, confirmed by the United States Secretary of the Department of Defense, Pete Hegseth, along with United States Senator Tom Cotton. https://lawenforcementtoday.com/bombshell-allegations-that-microsoft-using-chinese-employees-inside-china-to-oversee-dod-federal-government-cloud-infrastructure

I have personally been sounding the alarm on the Total Vote centralized software and the Microsoft Azure program for years and now we have confirmation from the federal government that our election infrastructure is at extreme risk.

In light of this explosive news, and the information provided in my recent complaint to the Government Operations and Audit Committee, I am requesting that every one of you take this issue seriously, and use all the power of the South Dakota State Government to investigate these issues, and to take appropriate actions to protect the government networks, voter data, and election night reporting systems.
https://www.sdcanvassing.com/_files/ugd/944eb0_d0d358b0d7e3434b90bfc620456927e3.pdf
Pennsylvania and Oregon have both terminated their $10 Million+ contracts with KNOWiNK Total Vote because of cyber security issues. Official documentation for both states list issues with the Microsoft Azure cloud and the inability to meet the cybersecurity requirements of the state. Third party independent project management oversight reports confirm KNOWiNK's failures to secure the data, resulting in terminated contracts and loss of millions of dollars of tax payer funds.

The Secretary of State of South Dakota has entered into a $4.5 Million contract with KNOWiNK for an updated program, which is currently and will be hosted on the compromised Microsoft Azure cloud platform, and is the same program that Pennsylvania and Oregon terminated their contracts for.

Friday, November 1, 2024 the State of South Dakota experienced a statewide outage of the Total Vote System, for which the Secretary of State still has not explained the cause or effects.

It is worth noting, all Elections Systems and Software (ES&S) computerized vote counting tabulators have a compromised supply chain, including Chinese microchips and motherboards.

This critical national infrastructure supply chain is compromised from its inception. It is also worth noting the State of South Dakota does not know who KNOWiNK is employing or subcontracting to work on government election infrastructure. Is anyone in the State of South Dakota certain foreign nationals are not being employed by or have access to the Total Vote System?

Also of note, Albert Sensor network devices are monitoring all South Dakota government internet traffic. These devices are "monitored" by an NGO called the Center for Internet Security, contracted by CISA. The DHS, CISA and CIS have been found to have weaponized their authority and it is all documented in congressional reports found here: https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/cisa-staff-report6-26-23.pdf https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/EIP_Jira-Ticket-Staff-Report-11-7-23-Clean.pdf

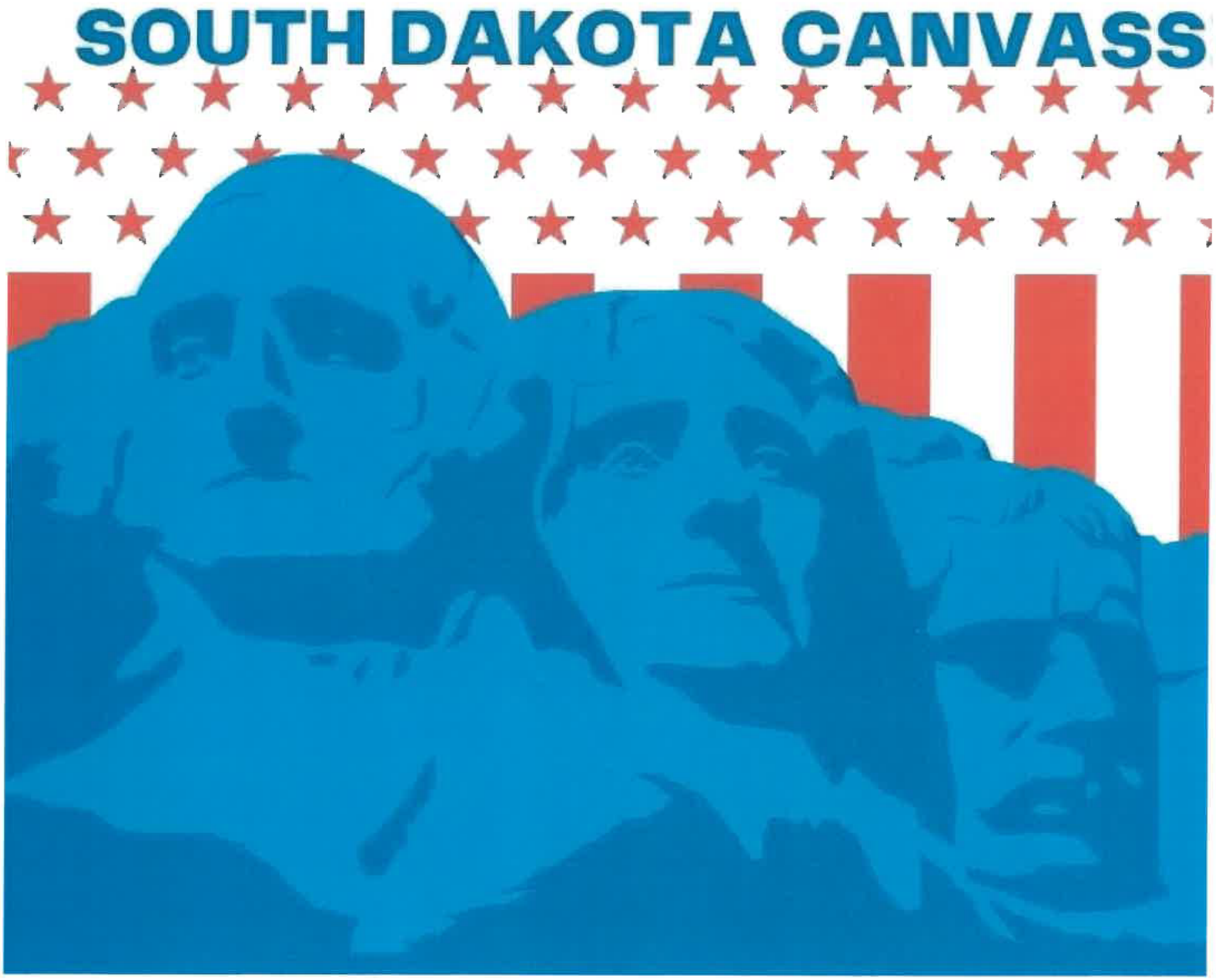
Albert Sensors also use the compromised Microsoft Azure Government platform, and were put into placed by rouge agencies found to have weaponized their authority in order to influence the outcome of a national election. Does the State of South Dakota consent to having all government internet traffic monitored by unknown NGO's and rogue federal agencies?

Governor Larry Rhoden has taken action to ban Chinese applications on government cell phones, and Former Governor and Secretary of Homeland Security, Kristi Noem has taken action to prevent Chinese ownership of United States farmland. I am requesting that you act immediately to secure our election infrastructure from Chinese influence or infiltration by immediately putting a halt to the KNOWiNK contract, implementing a review of all Microsoft Azure Government platforms, removal of Albert Sensor network monitors, and considering a ban on computerized electronic election equipment built with parts sourced in countries considered adversaries of the United States of America.

Thank you for your attention to this critical matter.

Sincerely,

[redacted]



Sent with Proton Mail secure email.