CYBERSECURITY THREATS IN THE STATES: RISK ASSESSMENT UPDATE

Recent cyber attacks on our nation's infrastructure, SolarWinds and Colonial Pipeline to name a few, have only become more severe and prevalent. The depth and reach of these types of threats, characterized by how hard they are to detect, requires coordination at all levels of government and the private sector. At the state level, these types of attacks have been used to access sensitive personal and financial information held by courts, police departments, elections departments, education departments, children and family services, and other social service providers and agencies. To assess the threat level in the states and raise awareness, **China Tech Threat** conducted an extensive research project based on Freedom Of Information (FOIA) requests and legal action to obtain information when necessary.

In 2019, China Tech Threat released a **report** on the failure of states to scrutinize the purchase of products and services from risky Chinese information technology vendors Lenovo and Lexmark which have been banned from U.S. military and intelligence networks for their connections with the Chinese government and military. The alarming fact is, despite being banned at the federal level, many states unwittingly still have purchase contracts with these dangerous companies. While federal policy directs information security for federal agencies, states determine their own information security standards. The research project was launched in conjunction with that report to identify the prevalence of state contracts with banned Chinese tech manufacturers. To date, this project revealed:

- There were **38** states with contracts with banned Chinese tech companies
- FOIA responses from nearly 30 states revealed more than **$50 million** spent on risky tech contracts
- **Even following formal legal requests, TN, ME and NJ** have yet to release information which could leave residents and infrastructure vulnerable to cyber threats

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) assert that People's Republic of China (PRC) state-sponsored cyber actors aggressively target U.S. political, economic, military, educational, and critical infrastructure personnel and organizations to steal sensitive data and intellectual property. America's use of electronics equipment and devices—many manufactured by PRC owned firms, represents yet another playing field for the PRC persist as a threat.

China Tech Threat's research process:

1. **Initial Analysis**: We did an analysis that identified 38 states with Lenovo and Lexmark contracts.
2. **FOIA Outreach**: In April 2020, a request was submitted to each state through their freedom of information laws stating we were aware of at least one contract with Lenovo and/or Lexmark, and requested any other available information about these companies dating back five years, including payments, orders, and equipment type purchased. Additionally, China Tech Threat requested an agency-by-agency purchase breakdown, when applicable.
3. **Assessing Threats and Alerting States**: Of the responses received by nearly 30 states, China Tech Threat analyzed the data, made it publicly available on our website and alerted members of the state's congressional delegation to the vulnerabilities and risks to state residents and infrastructure.
4. **Due Diligence**: Of the state's that failed to respond to the initial information requests, we continued outreach, sometimes through several attempts.
5. **Legal Action**: As of September 2021, six states had yet to respond and letters from our legal representative were then issued which prompted new information.

Today, Tennessee, **Maine** and **New Jersey** have yet to provide the information requested that could help state leaders identify and address cybersecurity risks in their state they may not even be aware of.

Next Steps: The only effective way to mitigate the risk of PRC intrusion is to restrict PRC products and services.

China Tech Threat will continue its analysis, outreach and communication to help raise awareness at the state level and help leaders identify and mitigate risk by reviewing their current contracts for security vulnerabilities. In doing so, they should ask two key questions:

- To what degree have state IT procurement leaders unwittingly put their citizens and enterprises at risk for intrusion by PRC actors by purchasing vulnerable equipment?
- To what degree have IT procurement leaders reviewed federal and state security and privacy laws to ensure that their purchase of vulnerable equipment complies?

At the federal level, China Tech Threat will continue its work to raise awareness of the role the National Association of State Procurement Officers (NASPO) can play in eliminating these threats. As the standard-bearer and leading state procurement conglomerate in the U.S. NASPO frequently negotiates contracts with large corporations for the purpose of validating product/service contracts for their members. Security is not currently a parameter of NASPO's evaluations, but should be incorporated into the contracting process.