Roslyn Layton, Ph.D.
957 8th Street South
Naples, FL 34102
roslyn@ChinaTechThreat.com

March 31, 2021

New York Office of General Services
Procurement Services
38th Floor, Corning Tower, ESP
Albany, NY 12242

Re: Lot 2, Aggregate Hardware Buy 20-01

VIA ELECTRONIC MAIL TO OGS.sm.PS.AggregateBuy@ogs.ny.gov

To Whom It May Concern,

I understand that the New York Office of General Services (OGS) seeks competitive quotations for Lot 2, Aggregate Hardware Buy 20-01.

As co-founder of the organization China Tech Threat which focuses on protecting Americans' privacy and security from technology products manufactured by companies owned and affiliated with the Chinese government, I have a few questions about your evaluation process. I kindly request your response which can be made public to the following questions.

1. **Does your evaluation consider the restrictions placed on specific vendors and technologies selected by U.S. military, intelligence, and other federal agencies?**

   A 2019 Department of Defense Inspector General (DODIG) report notes that Lenovo products have been restricted, investigated or deemed vulnerable by the DOD Information Network in 2018, the Joint Chiefs of Staff Intelligence Directorate in 2016, the Department of Homeland Security in 2015, and the State Department in 2006. Similarly, the DODIG notes that Lexmark has "connections to Chinese military, nuclear, and cyberespionage programs."

2. **How does your analysis consider the risk of purchasing equipment from adversarial nation state-owned enterprises, like companies owned by the governments of Russia, Iran, North Korea, and China?**

   Lenovo and Lexmark are companies with ownership by the Chinese government and companies who management has tied to the Chinese Communist Party. Consequently, they are subject to the intelligence law described below, therefore posing a privacy and security risk to New Yorkers.

3. **How do you evaluate data security?**

   As you may or may not know, the China's 2017 National Intelligence Law requires that companies based in China store data within country and allows for Chinese authorities to do 'spot-checks' on a company's network operations. Article 37 of the law specifically requires network operators in critical sectors to store data within mainland China that is gathered or produced by any Chinese operator.

   The transfer and storage of consumer data to mainland China introduces American users to the possibility of Chinese government data collection, compromising the data security and privacy of millions of New Yorkers.

After having conducted considerable research, I found that while federal policymakers have long focused on curtailing the security threats posed by Chinese-government owned technology firms, those same safeguards have not been adopted by state and local governments.

This problem is manifest in both (a) a lack of requisite security expertise within states and (b) a failure by the federal government to effectively convey their findings to state and local governments. There is significant information in the public domain describes the threat of Chinese government owned information technology. All the same, state governments continue to reward massive information technology contracts to vendors owned by the Chinese government. While it is not the intention of New York state government, these actions jeopardize the privacy and security of New York state residents and employees.

According to China Tech Threat's analysis, New York has spent more than any other US state on these two malign manufacturers in recent years: $14,882,890.20 on Lenovo computers, systems, and IT services; and $13,198,852.54 on Lexmark printers and related services. Learn more about these expenses at www.ChinaTechThreat.com/NY

I have much information on this topic, including a risk analysis of the aforementioned companies which I would be willing to share with you upon request. Please take seriously the responsibility of protecting all New Yorkers' privacy and security by preventing suspect information technology from your state's infrastructure.

Thank you for your attention to this matter.

Sincerely,

Roslyn Layton, Ph.D.
Co-Founder, China Tech Threat
roslyn@ChinaTechThreat.com