United States Senate
WASHINGTON, DC 20510

October 19, 2021

The Honorable Alejandro Mayorkas
Secretary of Homeland Security
Washington, DC 20528

Dear Secretary Mayorkas,

Like many of the Iowans we represent, we are concerned about the growing ransomware attacks in the nation's agricultural sector. The agricultural sector is designated as one of the country's sixteen critical infrastructure industries, but historically has not received robust cybersecurity support from the government.

NEW Cooperative, an Iowa grain cooperative, was recently targeted with a cyberattack. A Russian cybercrime cell, BlackMatter, took control of the Iowa co-op's systems and demanded $5.9 million. The systems BlackMatter attacked controlled crop irrigation, livestock feed schedules, and inventory distribution. NEW Cooperative controls 40% of the grain distribution in the country. The company's rapid return to alternative operations averted a crash in grain prices, but the threat of continued attacks has dire consequences.

In a separate cyberattack, BlackByte, another ransomware group, claims it attacked Farmers Cooperative Elevator Co., based in Arcadia, Iowa. BlackByte is threatening to release 100 gigabytes of sensitive data — including financial, sales and accounting information if a ransom isn't paid. With just four locations, Farmers Cooperative Elevator Co. is much smaller than NEW Cooperative.

The extent of the damage from the NEW Cooperative and Farmers Cooperative Elevator Co. attacks is not isolated to the grain market. Feed from the cooperatives' grain supply sustains millions of livestock. These attacks will affect the supply chain that puts food on the shelves in grocery stores across the country. As Iowa farmers adopt new technologies to get their crops to market, their exposure grows to similar attacks. That exposure not only risks the livelihood of Iowa farmers, it risks food security for Americans.

NEW Cooperative is only the latest in a long line of ransomware attacks against our critical infrastructure this year. In July, the Russia-linked group REvil attacked a Miami-based software provider, Kaseya, which resulted in trickle down effects to thousands of organizations that included Sweden's largest grocery chain. In June, the world's largest meat processing company, JBS, was attacked by REvil, shutting down nine meat packing plants in the United States. In May another Russian group, managed to shut down Colonial Pipeline for eleven days, resulting in buying panics and shortages. Now it seems clear that the group responsible for the Colonial Pipeline and NEW Cooperative attacks is the same Russian group with a new name.

In July, the Senate Judiciary Committee held a hearing about the threat of ransomware attacks from foreign countries with a permissive law enforcement policy. Eric Goldstein from CISA testified that the Joint Cyber Planning Office would be operating soon to identify and harden critical points of failure like NEW Cooperative. However, the Department of Homeland Security's current actions have clearly not deterred BlackMatter or shielded the agricultural industry.

The food supply chain and agricultural industry are critical to the wellbeing of all Americans. We would ask that you please respond to the questions below by November 19.

1. Explain how the Department of Homeland Security is integrating the agricultural sector into its preparations for future attacks.
2. What specific steps is DHS taking in responding to the NEW Cooperative attack and the resurgence of BlackMatter?
3. What resources is DHS leveraging to restore NEW Cooperative to a fully functional and secure state?
4. What programs are preparing our agricultural sector for future attacks?

Thank you for your consideration to this matter, we look forward to receiving your response. If you have any questions, feel free to reach out to us or our staff.

Sincerely,

Chuck Grassley
United States Senator

Joni K. Ernst
United States Senator