2022 POLICY GUIDES

Cybersecurity

ISSUE

The ability of a nation to feed itself is a matter of national security. As cyber threats grow, so does exposure to our members' operations and their supply chain partners. Those threats can ultimately impact our members' bottom lines, a loss of time and money, in a variety of ways (i.e., market manipulation by foreign nations, shut down of processing facilities, loss and sharing of individual farmer data to foreign nations, etc.).

Nebraska Farm Bureau (NEFB) can and should play a role in helping build awareness within our membership and across agriculture.

BACKGROUND

No matter where you live or work, one thing is true – cyber threats to our businesses, farms, food processing facilities, local governments, and communities in Nebraska is increasing exponentially. Today they are more pervasive and carry the potential for greater damage than ever before. We all need to be more proactive in working to detect, deter, and avert malicious cyber activity to protect our businesses and organizations from those who intend to cause harm.

Computer scientists and intelligence analysts must be ready to provide local expertise to prevent cyber-attacks from happening. Partnerships with the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) are crucial to ensure our safety, security, and confidence in a digitally connected world.

The threat is only increasing. There were supply chain attacks by Russia in 2020. The Chinese interfered with the Microsoft exchange server intrusions in 2021. And there have been ransomware attacks against agriculture coops, the energy sector, and major food processors such as JBS. There are incidents daily targeting businesses and other victims in our state, the rest of the country, and around the globe.

Nebraska is home to our nation's third largest agriculture complex. Ensuring the cybersecurity of one of our state and nation's most critical infrastructures – food production and distribution can only be done if we come together to develop the infrastructure, innovation, information, and systems we need to defend our livelihood in the private sector.

Early engagement is critical to success. We must work together against the threats affecting agriculture and food production. Our strategy must be multifaceted. We need to work with our partners such as the FBI and DHS to identify and target the bad actors, seeking to bring them to justice. We need to develop cyber protection and response plans.

In July, some of Nebraska Farm Bureau staff met with the FBI to discuss cybersecurity threats to our agriculture complex and how best to fight back. Due to escalating cybersecurity threats to agriculture businesses, the FBI wants to build relations with agriculture stakeholders to boost awareness of risks, while seeking input on how to work with

agriculture to mitigate financial losses through ransomware attacks (financial) and increase data protection (personal & national security).

The FBI is working in four key areas:

- Counterterrorism with emphasis on domestic terrorists such as animal rights extremists.
- Counterintelligence where the focus is on the theft of intellectual property (seed, genetics, data, and other ag technology) by North Korea, Iran, Russia, and China; and by those who wish to wreak havoc on our energy, food production, water systems, and transportation.
- Cybersecurity, because of the large concerns about vulnerabilities in agriculture due to the structure of our industry – i.e., many small businesses, using extensive supply/input chains, and largely independent in nature.
    - Ransomware is becoming an industry.
    - FBI has helped businesses recover ransomware dollars when contacted soon enough.
    - FBI is encouraging agricultural partners to strengthen preventative measures (i.e., dual factor authentication, offline backups, limiting administrative rights to data, etc.)
- Criminal activity (i.e., gangs, fraud – white collar crimes, crimes against children, etc.)

Next Steps

- The FBI is interested in getting in front of agricultural leaders to generate awareness and dialogue on cyber threats. They are interested in holding a conference/event to get leaders across agriculture together to exchange information.
- NEFB indicated a willingness to promote and help with some type of event (likely after harvest), including the development of a list of who should be invited.

FARM BUREAU POLICY

N/A

QUESTIONS

1. Should this be a high priority for NEFB?
2. How should NEFB lead in this space with solutions?
3. Who are our partners in fending off cyber-attacks and ensuring our cybersecurity?
4. What roles should federal, state, and local government play in this space?
5. What policy does NEFB need to guide our policy team when working in this area?