NEBRASKA FARM BUREAU®

2021 POLICY GUIDES

Cyber & Data Security In Agriculture

Issue/Background

The Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) recently released a report addressing increased threats to data security in the agricultural space. As more farmers and ranchers adopt precision agricultural techniques and move from mechanical to technological, they experience the benefits of increased productivity and the challenges of increased vulnerability due to more connections online. The report examined potential threats to confidentiality, integrity and availability and found that potential bad actions included: "data theft, stealing resources, reputation loss, destruction of equipment or gaining an improper financial advantage over a competitor." Unfortunately, as the recent cyberattack against JBS also demonstrated, these are not the only threats that exist. Upon gaining access, hackers could shut down production for hours or days at a time, modify machinery procedures to slow down production or even take machinery hostage in search of ransom payments. Not only do threats exist from malevolent individuals, but threats could also come from state actors. A hostile nation like China could use yield data, land prices or herd health data for purposes against the national security of the United States, or (perhaps more insidiously) simply replace the data with false data that would mislead producers.

In short, as more farmers and ranchers connect portions or all of their operations to web-connected technology, the threats to data security will become more prevalent. Nebraska Farm Bureau seeks your input on whether our current policies need to be updated to better protect against cyber threats and protect not only farmer and rancher data but also their operations.

Policy ideas:

1. Create educational programs at FDA/USDA and/or at the state level to promote good cybersecurity practices.
2. Create incentive programs in the form of grants to facilitate research into data security standards in agriculture and reward early adopters of cutting-edge cybersecurity practices in the industry.
3. Add the specific line item of "Data Security" or "Cybersecurity" to the name and jurisdiction of subcommittees of the House & Senate Agriculture Committee to elevate its importance.
   - Example: House Agriculture Subcommittee on General Farm Commodities, Data Security and Risk Management

Farm Bureau Policy

Nebraska Farm Bureau does not currently have a state policy on this topic, but a minimal AFBF policy does exist. 179 / National Security Line 2.8 Page 45 and 536/ Proprietary Data Pages 192-193.

BENEFITS

Increased awareness of the issue could lead to an increased focus on cyber issues at all levels of government and could also lead to more farmers and ranchers taking steps individually to protect their operations.

CONCERNS

Does government have any role to play in promoting cybersecurity? If so, what is the correct balance of government involvement in promoting cybersecurity without moving toward a government as a "data clearinghouse" which we have policy opposing?

QUESTIONS

1. Does the national policy currently adopted by Farm Bureau need to be updated to better emphasize the importance of cybersecurity with agricultural data?
2. What are other ways that Nebraska Farm Bureau and/or American Farm Bureau could increase awareness of this critical issue with farmers and ranchers and encourage them to be thinking about this?
3. Should Nebraska Farm Bureau enact policy specifically supporting any of the above ideas? Should NEFB take any of these policy ideas to the national level for consideration by AFBF?