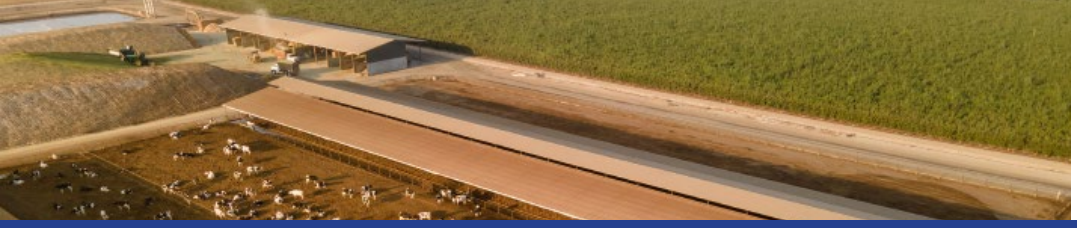
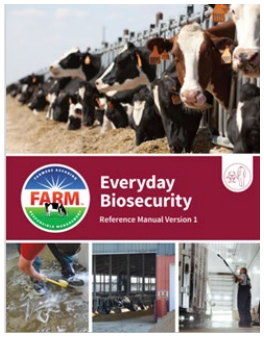


CDQAP Quality Assurance Update - November 2022

FARM Program Releases Everyday Biosecurity Manual

By Miquela Hanselman, Manager, Regulatory Affairs, National Milk Producers Federation

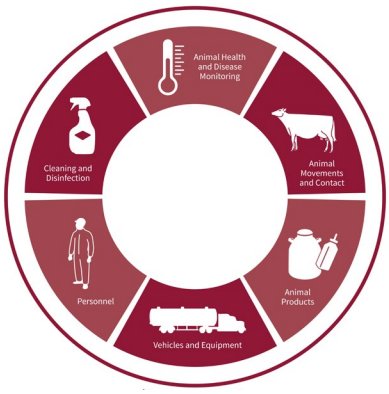


The National Dairy Farmers Assuring Responsible Management (FARM) Program has released the first Everyday Biosecurity manual. The manual outlines small, routine steps dairy farmers can take to protect the health of their herds and employees. FARM Biosecurity, launched in 2021, is FARM's newest program area and encompasses both everyday and enhanced biosecurity practices for voluntarily participation. Funded through USDA's National Animal Disease Preparedness and Response Program (NADPRP), FARM Biosecurity focuses on increasing awareness of biosecurity throughout the dairy industry by providing practical and effective steps to further promote cattle health. It complements the animal health and husbandry recommendations included in the FARM Animal Care, Drug Residue Prevention, and Environmental Stewardship Programs.

Biosecurity is a multi-step process and everyday biosecurity is the first step. Producers can get started by following simple measures outlined in the manual. There are seven areas to focus on—animal health and disease monitoring, animal movements and contact, animal products, vehicles and equipment, personnel, cleaning and disinfection, and a line of separation.

Putting these measures in place can prevent the introduction, detect the presence, and contain the spread of diseases, benefitting cattle and human health on farm. Everyday biosecurity practices protect against common diseases like contagious mastitis, respiratory infections, hairy foot warts, and scours. With effective everyday biosecurity steps, farmers can prevent or lessen the impact of these diseases on their cattle.

Enhanced biosecurity will be needed to protect cattle from a highly contagious Foreign Animal Disease (FAD), like Foot-and-Mouth Disease (FMD).



The FARM Biosecurity program incorporates the resources from the Secure Milk Supply (SMS) Plan for Continuity of Business during an FMD outbreak. The SMS Plan was developed in collaboration with industry, state and federal animal health officials, and academic partners with USDA funding, beginning in 2009. In an FMD outbreak, dairy farms located in a regulatory Control Area would need a movement permit issued by the state to ship cattle, semen, embryos, and possibly raw milk.

Continued on Page 2

Industry and Law Enforcement Partner on Cyberattacks

October webinar highlights resources processors can use to prevent ransomware attacks.

By Dr. Michael Payne, UC Davis, School of Vet. Medicine; Director, CDQAP

Cyberattacks traditionally involve a wide variety of targets. Schools and hospitals, retail and manufacturing companies, financial services and government agencies are all frequent victims. One report cited that in 2021 alone there were 2,566 U.S. ransomware victims, with an average demand for $2.2 million.

With increasing frequency however, agriculture has also become a target for cyber and ransomware attacks. Schreiber Foods dairy processing in Wisconsin experienced a $2.5 million dollar ransomware attack in 2021. That same year JBS meat packing paid $11 million dollars in ransom to REvil, a Russian-based ransomware group. Also in 2021, the Dairy Farm Group, one of the largest dairy retailers in Asia, suffered a ransomware attack demanding $30 million dollars. This year in the U.S., western dairy processing facilities also experienced cyberattacks.

Last month, a collaboration between the dairy industry and law enforcement cyber-experts delivered a unique webinar focusing on preventing and responding to cyberattacks. A wide variety of issues were addressed including descriptions of how cyber-attacks work, creating a cyber-emergency team and response plan, and the state and federal resources available to processors.

Every dairy processor in California was invited to participate in the webinar but, for security reasons, registration was required and the event was not recorded for later viewing. The California Milk Advisory Board hosted the virtual event, and all registrants were confirmed as dairy or law enforcement personnel prior to the meeting.

More than 50 attendees from four states attended the webinar. Companies in attendance ranged from large multi-state cooperatives to specialty glass-bottlers.

Continued on Page 2

Everyday Biosecurity Manual *continued*

The FARM Biosecurity Program is also developing an online option for producers, their veterinarian, and FARM evaluator to create an enhanced biosecurity plan ahead of an outbreak. Once put in place, cattle will be better protected against FMD and producers will be better positioned to meet the biosecurity movement permit requirement to move their cattle and products during a FAD outbreak.

Good biosecurity takes time and practice to be effective. Building these practices into your routine—or reinforcing the best management practices in the Everyday Biosecurity manual that you are already doing—can help protect animals from all kinds of diseases. This ultimately moves the industry one step closer to protecting cattle and the U.S. milk supply. More information is available at https://nationaldairyfarm.com/farm-biosecurity/. Questions? Contact mhanselmen@nmpf.org

The FARM Program was created by the National Milk Producers Federation in partnership with Dairy Management Inc. The FARM Program works with dairy producers, cooperatives, processors and industry partners through five program areas – animal care, antibiotic stewardship, biosecurity, environmental stewardship and workforce development – to show customers and consumers that the dairy industry holds itself to the highest standards and best management practices.

Industry and Law Enforcement Partner on Cyberattacks *continued*

and Hispanic cheese manufacturers. All four of California's dairy trade organizations were represented, as well as dairy organizations from Oregon and Washington.

Cybersecurity and physical security experts from four law enforcement agencies participated. Prior to the webinar thirteen of these security experts toured two major dairy processing plants in the Central Valley. This included experts from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the FBI, the California Cybersecurity Integration Center, and the Central California Intelligence Center (CCIC).

Highlights of the webinar included:

Threat Overview – The Center for Strategic and International Studies puts global losses to cybercrime at $1 trillion annually. Presenters including those from the Federal Bureau of Investigation (FBI) pointed out that all portions of the agriculture supply chain were susceptible. Numerous motives included not only ransomware, but industrial espionage and theft of trade secrets as well. In addition, employee information and credentials may be stolen for sale on the dark web. Vendor and billing information can be collected to perpetrate illicit transfers, wire fraud and other financial crimes.

A wide variety of threat actors are involved, including nation states, terrorists, hackers, cybercriminals, organized crime groups and competing companies. Research indicates that data breaches and ransomware aren't going to stop. More than a million new malware variants released each day. The greatest cybersecurity challenge to companies remains employees. Ninety percent of hacks and breaches originate with phishing emails.

Agency Coordination – Speakers from the Central California Intelligence Center (CCIC) described how the state's five Fusion Centers share information to prevent and respond to both physical and cyber crime threatening California farmers. Covered in detail was how network Vulnerability Assessment & Penetration Testing (VAPT) can be used to identify a company's greatest cyber risks. For companies new to or renewing cybersecurity efforts, CCIC is potentially their first contact for advice and referral.

Agency Resources – Experts from the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) and the California Cybersecurity Integration Center (Cal-CSIC) described the many resources available to industry. These include VAPT assessments, exercises, training, software scanning, threat alerts and incident reporting & response. Presenters focused on priority practices companies should be implementing and maintaining now including: 1) multi-factor authentication 2) resilient passwords 3) employee phishing training and 4) regular software scanning and updates.

For producers or processors interested in learning more on how to access cybersecurity resources or CDQAP's partnership with law enforcement partners, contact Dr. Michael Payne at mpayne@ucdavis.edu.