Testimony for the Record
Submitted to the
House Agriculture Committee
Subcommittee on Livestock and Foreign Agriculture

Jennifer van de Ligt, PhD

Director, Food Protection and Defense Institute
Associate Professor, College of Veterinary Medicine
University of Minnesota

Chairman Jim Costa and Ranking Member David Rouzer, and Members of the Subcommittee on Livestock and Foreign Agriculture, thank you for inviting me to participate in today's hearing. It is an honor to appear before you.

I am the Director of the Food Protection and Defense Institute and Associate Professor in the College of Veterinary Medicine at the University of Minnesota.

The Food Protection and Defense Institute (FPDI) at the University of Minnesota is an Emeritus Homeland Security Center of Excellence dedicated to providing leading-edge research, technical innovation, and education to protect the food system from disruption. Since 2004, FPDI has partnered with stakeholders across government, industry, NGOs, and academia to assure product integrity, supply chain resilience, and brand protection throughout the food and agriculture sector.

I have an extensive background in food defense, animal feed and human food production, human and animal nutrition, systems modeling, and scientific and regulatory affairs, with academic, industry, and global perspective. My academic career has focused on building collaborations to assure effective public-private partnership and stakeholder engagement to advance food and feed security, safety, defense, and supply-chain resilience. Prior to joining the University of Minnesota, I held numerous leadership positions at a multinational food company operating in 70 countries where I provided nutrition, regulatory, and scientific affairs expertise across their human food and animal feed portfolios. I have more than 130 global patents and patent applications covering specialty ingredients, processing technology, packaging innovations, and biology-based dynamic modeling formulation systems.

Background

Cyber risk is not new to the food and agriculture sector, but the risk of significant business disruption and significant national security threats from cyberattack are growing.[1] Traditional information technology (IT) in the form of email, data storage, records retention, and point of sale activities are ubiquitous and have been for many years. These systems are updated regularly with most food firms relying on in-house, or third-party, IT providers to manage cybersecurity for their systems.

The newer cyber risk in the food and agriculture sector is the growing dependence upon cyber-based information and operational technology (OT) systems used to perform an ever-expanding variety of normal operating procedures. The operational technology systems, including industrial control systems and internet-connected sensors, controllers, and devices (sometimes referred to as the internet of things or IOT), manage the most critical aspects of food production, typically have the lowest level of integrated cybersecurity protections, and are often not included in enterprise cybersecurity plans, protections, and training.

Two pieces of operational technology illuminate aspects of cyber risk in the food and agriculture sector. First, a pasteurizer in a fluid milk or juice manufacturing facility is critical to assuring the food safety of those products. The pasteurization time and temperature are controlled by sensors communicating with control systems monitored remotely by food safety professionals. Second, in beef harvest facilities, carcasses must be split into right and left halves prior to further processing. This splitting is increasingly being done by robotic carcass splitters. If either of these pieces of equipment are compromised through a cyberattack, the facility would be required to shut down and

[1] Food Protection and Defense Institute. 2019. Adulterating More Than Food: The Cyber Risk to Food Processing and Manufacturing. https://hdl.handle.net/11299/217703

economic consequences would result. Depending upon the type of cyberattack and the speed at which it is detected, other consequences may also occur. For example, if the pasteurizer is compromised, it may inaccurately, and possibly even maliciously, report and record that acceptable food safety metrics were reached – even though they were not – resulting in unsafe product being distributed and wide-scale human health harm. Cyberattack on the carcass splitter could result in serious worker injury to human operators present in those areas.

Although the above examples are hypothetical and used to illustrate types of technology at risk of cyberattack, the concept of cyberattack in the food and agriculture sector is not hypothetical. It has been occurring for years and is gaining recognition as a significant threat to business continuity and national security. In fact, Dragos, Inc. reported that ransomware attacks on industrial entities increased more than 500% from 2018 to 2020.[2]

History of cyber-attacks in the food and agriculture infrastructure

As early as 1998, cyber criminals targeted the food and agriculture sector with denial-of-service attacks, ecommerce thefts, and intellectual property thefts. However, most of these attacks had limited public exposure to avoid brand damage. The more recent cyberattacks have evolved to compromise networks, disrupt operations, and/or exfiltrate vast amounts of data. The scale of these recent attacks, in terms of ransoms paid and levels of operational disruption due to the significant consolidation across the sector, make such events difficult to keep from the public eye. To make matters worse, the rise of cryptocurrency payments to end the attack and recover data makes it exceptionally hard for law enforcement to identify the criminal organization and track and recover payments.

Since late 2020, major cyber incidents (e.g., SolarWinds, E&J Gallo, Molson Coors, Colonial Pipeline, JBS, Kaseya, and others) have severely disrupted the ability to conduct business for many companies in the food and agriculture sector. With many of these companies paying ransom to end the attack, it is likely that attacks will continue. In addition, the pandemic highlighted how food and agriculture sector consolidation and interdependencies increase not only risk of disruption but also the probability that accompanying publicity will result in increased targeting of food and agriculture sector infrastructure. Ransomware, data theft, and operational disruption are not the only issue. As shown with water treatment facilities in California and Florida, cyberattacks are also intended to harm health. In these attacks, water disinfection chemical levels were adjusted to harmful levels.

Implications of the growing cyber risk in the food and agriculture sector

The food and agriculture sector is incredibly diverse. It is composed of facilities ranging from small businesses and family farms to multinational corporations that produce an infinite variety of foods. Some aspects of the food and agriculture sector are highly distributed, while some are highly consolidated. Each and every business, farm, production facility, and company is individually vulnerable to cyberattack. On a broader scale, however, the food system is one of the most interconnected and interdependent systems within the critical infrastructures. Relationships among food companies can include supplier, customer, and competitor simultaneously. These interconnections often mean that data flows routinely and fluidly across the sector. From a cyber perspective, this amplifies the attack surface and the risk. It also amplifies the potential magnitude of system disruption and failure from a cyberattack, including its secondary and tertiary cascading impacts.

---

[2] Larson and Singleton. 2020. Ransomware in ICS Environments.

The food and agriculture sector is labor intensive. However, a history of labor shortages coupled with technology advancements have driven automation in the sector. The changing worker health provisions and expectations exacerbated by labor shortages during the pandemic have only accelerated the motivation within the food and agriculture sector to increase automation. However, with every advancement comes unintended consequences. With increased automation and the concomitant rise in computational and network complexity, cyber risk also increases.

Regardless of why cyber risk exists, cyberattacks have the potential to cause catastrophic disruption and endanger national security concerns. For example, the recent JBS cyberattack disrupted meat processing operations in several countries and simultaneously caused disruptions to supply chains, logistics, and transportation to customers. And it increased consumer prices. This amplification of disruption can easily result in national security threats depending upon the scale of attack and subsequent disruption.

As a hypothetical example of a national security threat, consider for a moment the impact if both of the only two HDPE pellet plants that produce the gallon milk jug preforms were the victims of a simultaneous cyberattack? We know that during Hurricane Katrina when just one of these HDPE facilities was compromised, the supply of fluid milk at the consumer level plummeted to shortage levels in many areas of the country while dairy farmers dumped millions of gallons of milk. A situation, such as this, could be repeated and affect a broad area of the nation in the event of a targeted cyberattack.

Our FPDI research and experience engaging with food system stakeholders led us to identify the following primary (but not exclusive) causes for cybersecurity risk to agricultural and food products supply chains:

- Lack of awareness throughout the sector of the scale of cybersecurity risks to agricultural and food processing and manufacturing and the potential consequences if those risks were realized.
- Lack of regulatory guidance and clarity regarding how cybersecurity risks should be accounted for and addressed in assessing food safety risks.
- Lack of standards for the cybersecurity of agricultural and food processing systems, both for the operation of those systems and for the design and development of the software and hardware that comprise them.
- Lack of research and vulnerability assessment data upon which to make evidence-based cybersecurity risk mitigation and policymaking decisions. This especially hampers the ability to prioritize the most vulnerable products or processes for mitigation efforts.
- Lack of cybersecurity education and training among operations technology personnel and lack of control systems knowledge among information technology personnel tasked with cybersecurity at agriculture and food companies. This is particularly acute at small- and medium-sized businesses.

It should also be recognized that although some food and agriculture sector partners may recognize the risk, constraints exist in their ability to manage that risk. They must balance a multitude of supply chain, food safety, labor, financial, and other operational risks in addition to cyber risk. Not only does managing cyber risk increase operational costs, but there are also very few experts with the knowledge and experience to effectively enhance cybersecurity in the food and agriculture operational environment. This type of expert is often recognized as irreplaceable and are sometimes referred to as 'unicorns' within the food industry. We need to train and field many more of them.

Recommendations for enhanced cyber resilience

Current federal law (the Food Safety Modernization Act) specifies that covered facilities must establish and implement a food safety system that includes an analysis of hazards and risk-based preventive controls. Regulations promulgated by FDA require a written food safety plan that includes steps for hazard analysis, preventive controls, oversight and management of preventive controls, monitoring, corrective actions, and verification. Few of these steps can be undertaken without information technology, industrial control systems, and internet-based communication systems. Any compromise of these supporting systems jeopardizes implementation of these critical food safety procedures, including the process controls that must be addressed in hazard analysis and protective strategies, as well as others such as product testing and environmental monitoring. In addition, more historical FDA regulations address electronic records creation, accuracy, and retention. However, aspects of the food and agriculture sector may not be covered by these regulations (e.g., USDA-regulated food facilities, farm-level production, etc.) and none of the current regulations address cybersecurity of the systems required to acquire, manage, and preserve these records.

As provided in the FPDI comments offered in response to "Notice: Supply Chains for the Production of Agricultural Commodities and Food Products, Request for Public Comments", I, as Director of FPDI, recommend the following actions:

- USDA should take the lead in developing new minimum information technology risk reduction regulations and develop new Good Manufacturing Practices (GMPs) specific to the production agriculture and food and beverage industries. These could be developed as a new set of cyber preventive controls to be consistent with the implementation of other Food Safety Modernization Act (FSMA) requirements. This action should be taken in concert with industry, the Department of Homeland Security (DHS), the Food and Drug Administration (FDA), and the Federal Bureau of Investigation (FBI).
- USDA, in collaboration with FDA, should develop sector-specific system risk reduction measures, facility-level cybersecurity risk reduction plans, and operator guidelines and training. They should also develop specific preventive controls training and reporting for cyber systems within the food and agriculture sector.
- USDA should host a series of cybersecurity review and technology forums or similar events for food and agriculture sector senior management to accelerate the education of senior leadership within industry. Senior leadership needs a better understanding of the cyber risks and the importance of investing in risk reduction for cyber systems, especially in the food and agriculture operating environment. This action should occur in partnership with the insurance industry, the cybersecurity industry, FDA, FBI, and DHS,
- USDA should develop a university-based food and agriculture sector focused cyber Center of Excellence to conduct research and education that aids in cyber risk reduction.
- USDA should collaborate with industry and DHS to establish an Information Sharing and Analysis Center (ISAC). The mission of this ISAC should be to understand evolving food and agriculture sector cyber risks as they may impact both individual facilities and entire supply chains, anticipate local and broad supply chain exposures, and monitor cyber technology shifts and emerging cyber-based or control technology risks across all aspects of the food system.

Closing Remarks

Securing the vast cyberinfrastructure and electronic information systems sustaining America's food and agriculture supply system is vital to the economic vitality of the system and our nutritional and

national security. If we do not act, we risk the nation's ability to provide a sufficiency of nutrition, the very essence of well-being for our friends, family, colleagues, constituents and institutions.

I, and the Food Protection and Defense Institute, appreciate the opportunity to engage in and contribute to this national discussion of our food system's resilience.

Thank you. I look forward to further discussion on this important topic.

Jennifer van de Ligt, PhD

Minneapolis, MN • jennifer@vandeligt.net • (763) 350-5687 • www.linkedin.com/in/j-van-de-ligt/

Education

Ph.D.	University of Kentucky	Nutrition – Monogastric
M.S.	University of Illinois	Nutrition – Ruminant
B.S.	North Carolina State University	Animal Science (nutrition minor)

Career Progression

University of Minnesota (2016 – present)

Associate Professor Veterinary Population Medicine (2018 – present)

Director Food Protection and Defense Institute (2019 – present)

Director Integrated Food Systems Leadership Program (2018 – present)

Director of Graduate Studies Applied Sciences Leadership (2020 – present)

- Revamped and lead Food Protection and Defense Institute research and outreach programs promoting national health security; food systems, security, and defense; supply chain resilience; and prevention of intentional adulteration of food
- Designed, launched, and lead Integrated Food Systems Leadership Regents Certificate Program and Applied Sciences Leadership Master of Professional Studies to grow leaders to feed the future with a focus on feeding the world sustainably through full utilization of the agricultural toolbox
- Lead cross-functional, multi-collegiate research team investigating transboundary animal disease mitigation through development and application of novel model systems with public-private partnership sponsorship
- Build partnerships with public and private sector stakeholders
- Lead programmatic advisory boards to create and implement strategic plans for research programs and outreach initiatives
- Achieve specific and measurable research and outreach goals, promote research excellence through peer review, utilize financial resources effectively, and set and achieve revenue expectations
- Supervise, mentor, and align talented staff dedicated to improving the food system with an emphasis on national health security, sustainability, and food protection through research, education, and translation to application
- Promote University, College, Department, Program, and Institute at national and international conferences, forums, and meetings

ToxStrategies, Inc. (2018 – present)

Senior Consultant

- Identify and execute food and nutrition regulatory interpretation and strategy, ingredient safety, and new ingredient approval for client products and portfolios

Cargill, Incorporated (1999 – 2016)

Associate Director Scientific and Regulatory Affairs (2012 – 2016)

- Led team that developed extramural safety and efficacy research strategy; created and implemented scientific affairs and advocacy, claims and labeling, and regulatory plans; consulted with regulatory authorities to open markets for new food ingredients
- Directed and mentored technical team, including external consultants, to grow the value of the team as a trusted advisor and essential business partner
- Partnered with federal and international governmental stakeholders, leading science foundations, multi-national food manufacturers, targeted trade associations and external stakeholders to proactively influence public policy, nutrition, and regulatory modernizations
- Updated strategic direction, and negotiated and managed budget for North American Scientific & Regulatory Affairs

Senior Manager Regulatory and Scientific Affairs (2007 – 2012)

- Opened key international markets for Truvia® sweetener products through global collaboration, development of regulatory guidance, scientific substantiation for product claims, and management of regulatory risks.
- Customized regulatory strategy for variety of health, nutrition, and functional human food ingredients through partnership with business leadership, product development, marketing and sales, and legal teams
- Secured funding and initiated multi-year research program to substantiate nutritional and health efficacy of functional ingredient in healthy populations

Intellectual Asset and Innovation Development Manager (1999 – 2007)

- Established intellectual asset management strategy to enhance competitive advantage for global animal nutrition business in collaboration with senior leadership
- Optimized strategic development of branded, novel, and patent-pending ingredients to meet nutritional composition, regulatory compliance, and processing conditions in cross-functional, cross-cultural, and multi-site extramural team environments

Recognition

2021-22 University of Minnesota – University Senate Health Sciences Faculty Consultative Council

2020-24 University of Minnesota – College of Veterinary Medicine Faculty Consultative Council

2020-22 University of Minnesota – Healthy Food Healthy Lives Advisory Board
2020-22 University of Minnesota – Consortium of Law and Values Advisory Board
2018-22 University of Minnesota Toxicology Program – Advisory Board
2016-22 Institute of Food Technologists – Global Food Traceability Center Advisory Board

Publications (select)

Shurson, G. C., Urriola, P. E., & **van de Ligt, J.** (2021). Can we effectively manage parasites, prions, and pathogens in the global feed industry to achieve One Health? Transboundary and emerging diseases, 10.1111/tbed.14205. Advance online publication. https://doi.org/10.1111/tbed.14205.

Shurson, G. C., Palowski, A., **van de Ligt, J.**, Schroeder, D. C., Balestreri, C., Urriola, P. E., & Sampedro, F. (2021). New perspectives for evaluating relative risks of African swine fever virus contamination in global feed ingredient supply chains. Transboundary and emerging diseases, 10.1111/tbed.14174. Advance online publication. https://doi.org/10.1111/tbed.14174.

Fitch, S.E., Payne, L.E., **van de Ligt, J.L.G.**, Doepker, C., Handu, D., Cohen, S.M., Anyangwe, N, and Wikoff, D. (2021). Use of acceptable daily intake (ADI) as a health-based benchmark in nutrition research studies that consider the safety of low-calorie sweeteners (LCS): a systematic map. BMC Public Health 21, 956. https://doi.org/10.1186/s12889-021-10934-2.

van de Ligt, J.L.G., S. J. Borghoff, M. Yoon, L. J. Ferguson, W. DeMaio, and R. H. McClanahan. 2019. Nondetectable or minimal detectable residue levels of N-(n-butyl) thiophosphoric triamide in bovine tissues and milk from a 28-d NBPT dosing study. Trans Anim Sci. 3:4, 1606-1616. https://doi.org/10.1093/tas/txz153

Crincoli, M. C., V. Garcia-Campayo, M. O. Rihner, A. I. Nikiforov, D. Liska, J.**L.G. van de Ligt**. 2016. Evaluation of the gastrointestinal tolerability of corn starch fiber, a novel dietary fiber, in two independent randomized, double-blind, crossover studies in healthy men and women. Intl J Food Sci Nutr. 67:7, 844-56. http://dx.doi.org/10.1080/09637486.2016.1198891

Crincoli, M. C., A. I. Nikiforov, M. O. Rihner, E. A. Lambert, M. A. Greeley, J. Godsey, A. K. Eapen, J.**L.G. van de Ligt**. 2016. A 90-Day Oral (Dietary) Toxicity and Mass Balance Study of Corn Starch Fiber in Sprague Dawley Rats. Food Chem Tox. 97:57. http://dx.doi.org/10.1016/j.fct.2016.08.030

Patent Portfolio (US only issued and applications)

- System and method for optimizing animal production based on environmental nutrient inputs – US7827015
- System and method for optimizing animal production based on empirical feedback – US7904284
- System and method for optimizing animal production – US 2011/0010154, US 2008/0189085

- System and method for optimizing animal production based on dynamic nutrient information – US 2008/0154568, US 2006/0041413
- System and method for optimizing animal production based on empirical feedback – US 2008/0183453, US 2006/0041412
- System and method for optimizing animal production based on a target output characteristic – US 2008/0234995, US 2006/0041419
- System and method for optimizing animal production using genotype information – US 2007/0026493
- System and method for animal production optimization – US 2008/0189085, US 2006/0036419
- Stabilized pancreas product – US7153504
- Mineral feed supplement – US8993038
- High fat/fiber composition – US 2003/0170371
- Reclosable animal feed container – US 2009/0017172
- Solvent extracted corn – US 2008/0118626
- Corn based feed product – US 2007/092821

Truth in Testimony Disclosure Form

In accordance with Rule XI, clause 2(g)(5)* of the *Rules of the House of Representatives*, witnesses are asked to disclose the following information. Please complete this form electronically by filling in the provided blanks.

Committee: Agriculture

Subcommittee: Livestock and Foreign Agriculture

Hearing Date: 07/28/2021

Hearing Title :

State of the Beef Supply Chain: Shocks, Recovery, and Rebuilding

Witness Name: Jennifer van de Ligt

Position/Title: Director

Witness Type: ○ Governmental ● Non-governmental

Are you representing yourself or an organization? ○ Self ● Organization

If you are representing an organization, please list what entity or entities you are representing:

Food Protection and Defense Institute

FOR WITNESSES APPEARING IN A NON-GOVERNMENTAL CAPACITY

Please complete the following fields. If necessary, attach additional sheet(s) to provide more information.

Are you a fiduciary—including, but not limited to, a director, officer, advisor, or resident agent—of any organization or entity that has an interest in the subject matter of the hearing? If so, please list the name of the organization(s) or entities.

No

Please list any federal grants or contracts (including subgrants or subcontracts) related to the hearing's subject matter that you, the organization(s) you represent, or entities for which you serve as a fiduciary have received in the past thirty-six months from the date of the hearing. Include the source and amount of each grant or contract.

Although FPDI has received many federally funded grants beginning with its inception in 2004 as a Department of Homeland Security Center of Excellence, those related to the hearing's subject matter in the previous thirty-six month time period are:

2017-19. Vulnerability Assessment Framework. United States Department of Agriculture Food Safety and Inspection Service. FSIS-C-32-2017.$253,164.
2019. Basic Food Defense Training. Federal Bureau of Investigation Weapons of Mass Destruction Directorate. DJF-16-1200-D-0001479. $45,356

Please list any contracts, grants, or payments originating with a foreign government and related to the hearing's subject that you, the organization(s) you represent, or entities for which you serve as a fiduciary have received in the past thirty-six months from the date of the hearing. Include the amount and country of origin of each contract or payment.

None

Please complete the following fields. If necessary, attach additional sheet(s) to provide more information.

☑ I have attached a written statement of proposed testimony.

☑ I have attached my curriculum vitae or biography.

* Rule XI, clause 2(g)(5), of the U.S. House of Representatives provides:

(5)(A) Each committee shall, to the greatest extent practicable, require witnesses who appear before it to submit in advance written statements of proposed testimony and to limit their initial presentations to the committee to brief summaries thereof.

(B) In the case of a witness appearing in a non-governmental capacity, a written statement of proposed testimony shall include—(i) a curriculum vitae; (ii) a disclosure of any Federal grants or contracts, or contracts, grants, or payments originating with a foreign government, received during the past 36 months by the witness or by an entity represented by the witness and related to the subject matter of the hearing; and (iii) a disclosure of whether the witness is a fiduciary (including, but not limited to, a director, officer, advisor, or resident agent) of any organization or entity that has an interest in the subject matter of the hearing.

(C) The disclosure referred to in subdivision (B)(iii) shall include— (i) the amount and source of each Federal grant (or subgrant thereof) or contract (or subcontract thereof) related to the subject matter of the hearing; and (ii) the amount and country of origin of any payment or contract related to the subject matter of the hearing originating with a foreign government.

(D) Such statements, with appropriate redactions to protect the privacy or security of the witness, shall be made publicly available in electronic form 24 hours before the witness appears to the extent practicable, but not later than one day after the witness appears.