United States Government Accountability Office

Report to Congressional Addressees

November 2026

CRITICAL INFRASTRUCTURE PROTECTION

Further Action Needed to Enhance Cybersecurity of the Food and Agriculture Sector

GAO-27-108656

GAO Highlights

CRITICAL INFRASTRUCTURE PROTECTION

Further Action Needed to Enhance Cybersecurity of the Food and Agriculture Sector

GAO-27-108656 November 2026

A report to congressional addressees

Contact: David B. Hinchman at Hinchmand@gao.gov

What GAO Found

Increased use of technologies in the food and agriculture sector has made the sector more vulnerable to cybersecurity incidents, such as ransomware attacks. For example, a 2021 ransomware attack on a global meat processing company shut down some of the world's largest slaughterhouses and caused a shortage in meat supplies in the U.S. and other countries.

The U.S. Department of Agriculture (USDA) and the Department of Health and Human Services' Food and Drug Administration (FDA), as agencies primarily responsible for federal efforts to enhance the sector's cybersecurity, have taken a number of actions to improve the cybersecurity of the sector, but key steps remain. The agencies met most of the cyber-related aspects of the16 requirements under the six categories in the Fiscal Year 2021 National Defense Authorization Act, such as sector coordination, but only partially met or did not meet five requirements in the areas of information sharing and emergency preparedness aimed at better mitigating cybersecurity risks and attacks in the sector.

Extent to Which Sector Risk Management Agencies Have Met Requirements for Food and Agriculture Sector Cybersecurity

Category of requirement	Number of requirements	USDA	FDA
Sector coordination	3	● ● ●	● ● ●
Risk management	2	● ●	● ●
Risk assessment	2	● ●	● ●
Information sharing	4	● ● ● ◐	● ● ● ◐
Incident management	2	● ●	● ●
Emergency preparedness	3	● ◐ N/A	◐ ○ N/A

● = Met ◐ = Partially met ○ = Not met **N/A** = Not applicable

Sources: GAO analysis of Fiscal Year 2021 National Defense Authorization Act; and U.S. Department of Agriculture (USDA) and Food and Drug Administration (FDA) data. I GAO-27-108656

Both agencies reported that a lack of resources and staffing hindered their ability to meet all the requirements. By assessing whether there are opportunities to reprioritize or if there is a need for additional resources, the agencies would be better positioned to provide cybersecurity-related assistance and resources to the sector and help mitigate potential disruption of the food supply chain, which could lead to significant economic and environmental impacts.

In addition, selected private sector organizations reported actions to improve the cybersecurity of the sector, including sharing cyber alerts and distributing guidance to their members. The organizations also shared their views on opportunities and challenges to improve cybersecurity in the sector, including an increased need for collaboration between federal agencies and sector members.

Why GAO Did This Study

The food and agriculture sector is one of the nation's 16 critical infrastructure sectors and is essential to the nation's health, security, and economy. The sector is reliant on information technology to produce, process, and deliver products, and faces increasing cybersecurity-related risks. Cyberattacks could result in unsafe food and could erode public trust and faith in the food supply.

In this report, GAO (1) describes the potential cybersecurity risks to the sector; (2) evaluates the extent to which responsible federal agencies have taken actions to improve the cybersecurity of the sector; and (3) describes selected private sector organizations' actions and views to improve the cybersecurity of the sector.

GAO summarized publicly available information on cyberattacks impacting the sector. GAO analyzed actions taken by USDA and FDA to improve the cybersecurity of the sector and compared them to the 16 requirements in the Fiscal Year 2021 National Defense Authorization Act. GAO interviewed relevant federal officials and a nongeneralizable sample of six private sector organizations comprising a cross section of the sector.

What GAO Recommends

GAO is making three recommendations to the Department of Health and Human Services and two recommendations to USDA to fully implement cyber-related aspects of information sharing and emergency preparedness requirements and assess whether resources should be reprioritized or requested to do so. HHS agreed with its recommendations. USDA disagreed with its two recommendations, and requested GAO remove or redirect them. GAO continues to maintain that the recommendations are warranted.

Contents

Letter 1

Background 5
The Food and Agriculture Sector Faces Increasing Cybersecurity Risks and Has Experienced Cyberattacks 13
USDA and FDA Actions Met Most Cyber-Related Aspects of SRMA Requirements, But Key Steps Remain 17
Selected Private Sector Organizations Described Actions and Views to Improve FA Sector Cybersecurity 25
Conclusions 30
Recommendations for Executive Action 30
Agency Comments and Our Evaluation 31

Appendix I Comments from the Department of Heath and Human Services 35

Appendix II GAO Contact and Staff Acknowledgments 37

Tables

Table 1. National Defense Authorization Act of 2021 Requirements for Sector Risk Management Agencies (SRMA) 12
Table 2: Examples of Cybersecurity Threat Actors 14
Table 3: Examples of Publicly Reported Cybersecurity Attacks in the Food and Agriculture Sector, 2021 to 2026 16
Table 4. Extent to Which Sector Risk Management Agencies (SRMA) Have Met Requirements for Food and Agriculture Sector Cybersecurity 17

Figures

Figure 1. Stages in the Food Supply Chain 7
Figure 2. Technologies Used in Precision Agriculture 9

Abbreviations

CIPAC	Critical Infrastructure Partnership Advisory Council
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
FA	Food and Agriculture
FDA	Food and Drug Administration
FMIS	Farm Management Information System
GPS	global positioning system
HHS	Department of Health and Human Services
ISAC	Information Sharing and Analysis Center
IT	information technology
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NSM	National Security Memorandum
SRMA	sector risk management agency
USDA	U.S. Department of Agriculture

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

November 19, 2026

The Honorable Andrew R. Garbarino
Chairman
Committee on Homeland Security
House of Representatives

The Honorable Robert Garcia
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

Cyberattacks pose increasing risks to the nation's food and agriculture (FA) sector, which is a significant part of the U.S. economy. The FA sector is reliant on information technology (IT) to produce, process, and deliver products. However, cyberattacks on these technologies can lead to service disruptions that harm public health or the environment. For example, a cyberattack could override systems that monitor and control automated processes, leading to crops that are underwatered, overwatered, or improperly fertilized or unsafe production of food products. Cyberattacks resulting in unsafe food—or even the perception of unsafe food—can also erode public trust and faith in the food supply.

The U.S. Department of Agriculture (USDA) and the Department of Health and Human Services (HHS), acting through the Food and Drug Administration (FDA), are joint federal leads for the FA sector, referred to as sector risk management agencies (SRMA). As such, USDA and FDA are responsible for coordinating cybersecurity efforts with other federal agencies and private sector organizations that comprise the FA sector.

Protecting the cybersecurity of critical infrastructure has been part of GAO's High Risk List since 2003.[1] In September 2018, we issued an update to the High Risk List that identified actions that federal agencies needed to take to address cybersecurity challenges that the nation faces.[2] We later identified ensuring the nation's cybersecurity as one of nine High

[1]We first designated information security as a government-wide High Risk area in 1997. In 2003, we expanded this area to include cyber critical infrastructure protection. See GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas,* GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

[2]GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation,* GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

Risk areas that need especially focused executive and congressional attention.[3] We continue to identify the cybersecurity of critical infrastructure as a component of the cybersecurity High Risk area, as reflected in our biennial High Risk updates on major cybersecurity challenges.[4]

We performed our work at the initiative of the Acting Comptroller General. This report 1) describes the potential cybersecurity risks to the FA sector; 2) evaluates the extent to which responsible federal agencies have taken actions to improve the cybersecurity of the FA sector; and 3) describes selected private sector organizations' actions and views on ways to improve the cybersecurity of the FA sector.

To address the first objective, we summarized reports obtained from the Food and Agriculture Information Sharing and Analysis Center (Food and Ag-ISAC) regarding ransomware attacks against the FA sector.[5] We also obtained public information on cyberattacks that impacted the FA sector over the last five years. To do so, we conducted a literature search for information on cybersecurity-related threats and incidents to the FA sector, including publicly available information on cyberattacks and the impacts of such attacks. We searched for relevant publications during the period of January 2016 to January 2026 in the following databases: EBSCO, ProQuest, Scopus, and Lexis Nexis Secondary sources. We reviewed the literature to assess the quality of information, then summarized the relevant public reports, threat advisories, and other related documentation. In addition, we interviewed federal officials from USDA, FDA, and the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency's (CISA); and officials from six private sector organizations to identify potential cyber-related threats, vulnerabilities, and consequences of these threats and

[3]GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas,* GAO-19-157SP (Washington, D.C.: Mar. 6, 2019).

[4]GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges,* GAO-21-288 (Washington, D.C.: Mar. 24, 2021); *Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure,* GAO-23-106441 (Washington, D.C.: Feb. 7, 2023); and *High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation*, GAO-24-107231 (Washington, D.C.: June 2024).

[5]The Food and Ag-ISAC provides threat intelligence, analysis, and security practices that help food and agriculture companies detect attacks, respond to incidents, and share threat indicators so they can better protect themselves and manage risks to their companies and the sector.

vulnerabilities to the FA sector. The private sector organizations are discussed below.

To address the second objective, we identified SRMAs' requirements for coordinating activities specified in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Fiscal Year 2021 NDAA).[6] The 16 requirements in the act fall into these six categories: sector coordination, risk management, risk assessment, information sharing, incident management, and emergency preparedness. While the 16 requirements entail addressing all types of risks to critical infrastructure, we focused on efforts to address cybersecurity-related risks. In addition, we identified requirements from National Security Memoranda (NSM)-16[7] and NSM-22[8] to, among other things, develop annual risk assessments and biennial risk management plans for the sector.[9] We analyzed documentation from the co-SRMAs for the FA sector, USDA and FDA, to identify actions taken to improve the cybersecurity of the sector. For example, we analyzed the co-SRMAs'

[6]Section 9002(a)(7) of The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Fiscal Year 2021 NDAA, substituted the term "Sector Risk Management Agency" for "Sector-Specific Agency" in the definitions in section 2201(5) of the Homeland Security Act of 2002 (6 U.S.C. § 651(5)). Pub. L. No. 116-283, Div. H, Title XC, § 9002, 134 Stat. 4765, 4768 (2021). Section 9002 also made conforming amendments and other changes to critical infrastructure sector designation elsewhere in the Homeland Security Act. See 6 U.S.C. § 652a. The NDAA also added a new section, Section 2215 Sector Risk Management Agencies, that includes the responsibilities of those agencies, to the Homeland Security Act. Codified at 6 U.S.C. § 665d; see also, 15 U.S.C § 272(e)(3)(B) for definitions of "critical infrastructure" and 42 U.S.C. § 5195c(e), "Sector-Specific Agency" (now Sector Risk Management Agency) applicable to the National Institute of Standards and Technology's (NIST) responsibilities.

[7]The White House, *National Security Memorandum on Strengthening the Security and Resilience of United States Food and Agriculture*, National Security Memorandum 16 (NSM-16) (Washington, D.C.: Nov. 10, 2022). Although the NSM is under review, its requirements are still valid as Executive Order 14239 did not explicitly rescind the NSM.

[8]The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience*, National Security Memorandum 22 (NSM-22) (Washington, D.C.: Apr. 30, 2024). Although the NSM is under review, its requirements are still valid as Executive Order 14239 did not explicitly rescind the NSM.

[9]The March 18, 2025, Executive Order "Achieving Efficiency Through State and Local Preparedness" has placed NSM-16 and NSM-22 under review. According to Executive Order 14239, the memoranda were to be reviewed and recommended for revisions, recissions, and replacements within 180 days of the order. However, as of September 2026, no modifications to the memoranda had been proposed or issued. Therefore, the memoranda outlining sector risk management agency responsibilities are still valid as Executive Order 14239 did not explicitly rescind the NSM. Exec. Order No. 14239, 90 Fed. Reg. 13267 (Mar. 18, 2025).

2023 *120-Day Food and Agriculture Interim Risk Review*,[10] the draft *Food and Agriculture Sector Risk Management Plan*,[11] and joint cybersecurity advisories. We further reviewed USDA's and FDA's web pages to confirm that they offered resources online to food and agriculture organizations and obtain and analyze documentation that officials stated were available. We also validated with relevant officials that the websites and the available documentation were valid and current as of September 2026.

We then compared these actions and documentation to the 16 requirements in the Fiscal Year 2021 NDAA. For both USDA and FDA, we assessed the implementation of the requirements as follows:

- **Met.** We determined that a requirement was met if the agency demonstrated all aspects of the requirement.
- **Partially met.** We determined that a requirement was partially met if the agency demonstrated some aspects of the requirement.
- **Not met.** We determined that a requirement was not met if the agency did not demonstrate any aspects of the requirement.
- **Not applicable.** We determined that a requirement was not applicable.

In addition, we reviewed documentation from CISA, as the lead federal agency for cybersecurity, about coordination with USDA and FDA on sector cybersecurity. We further obtained written responses from federal agencies and interviewed relevant officials to obtain their perspectives on actions taken to improve sector cybersecurity.

To address the third objective, we selected a nongeneralizable sample of private sector organizations that comprise a cross section of the FA sector, such as trade associations in the grain, dairy, and meat industries. To select these organizations, we created a list of 85 members of the Food and Agriculture Sector Coordinating Council and narrowed it down

[10]Department of Health and Human Services, U.S. Department of Agriculture, and Department of Homeland Security, *National Security Memorandum on Strengthening the Security and Resilience of United States Food and Agriculture: 120-Day Food and Agriculture Interim Risk Review* (Washington, D.C.: Mar. 2023).

[11]U.S. Food and Drug Administration, and U.S. Department of Agriculture, *Food and Agriculture Sector Risk Management Plan* (Washington, D.C.: forthcoming). The forthcoming risk management plan was completed and submitted to the National Security Council and CISA in early January 2025. However, according to USDA and FDA officials, they have not received any comment or feedback since submitting the plan due to Executive Order 14239 ordering the review of NSM-22.

to 25 trade associations and organizations that have members and comprise a cross section of the sector.

Next, we sent that list to the Food and Ag-ISAC, which agreed to initiate contact with its members to see who would be willing to speak to us. The Food and Ag-ISAC put us in contact with officials from the National Chicken Council, the National Grain and Feed Association, and the Meat Institute. The officials from those organizations also put us in contact with the Food Marketing Institute and the Retail and Hospitality ISAC.[12] We also included the Food and Ag-ISAC as part of our sample. The six selected private sector organizations cover all stages of the food supply chain: production (farming/growing), processing/manufacturing, distribution (logistics/transport/storage), and marketing/retail/consumption.

We interviewed officials from the six selected organizations about actions taken to improve the sector's cybersecurity. We also obtained their views on challenges they have faced in collaborating with responsible federal agencies to identify and mitigate cybersecurity threats to the sector. We then analyzed responses from all six interviews and grouped the responses into categories such as threats/risks to the sector, federal and private sector cybersecurity coordination efforts, challenges, and ways to make improvements.

We conducted this performance audit from July 2025 to November 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The U.S. critical infrastructure refers to the systems and assets, whether physical or virtual, so vital to the U.S. that their incapacity or destruction would have a debilitating impact on our nation's security, economic stability, public health or safety, or any combination of these factors. National policy has identified 16 critical infrastructure sectors, including

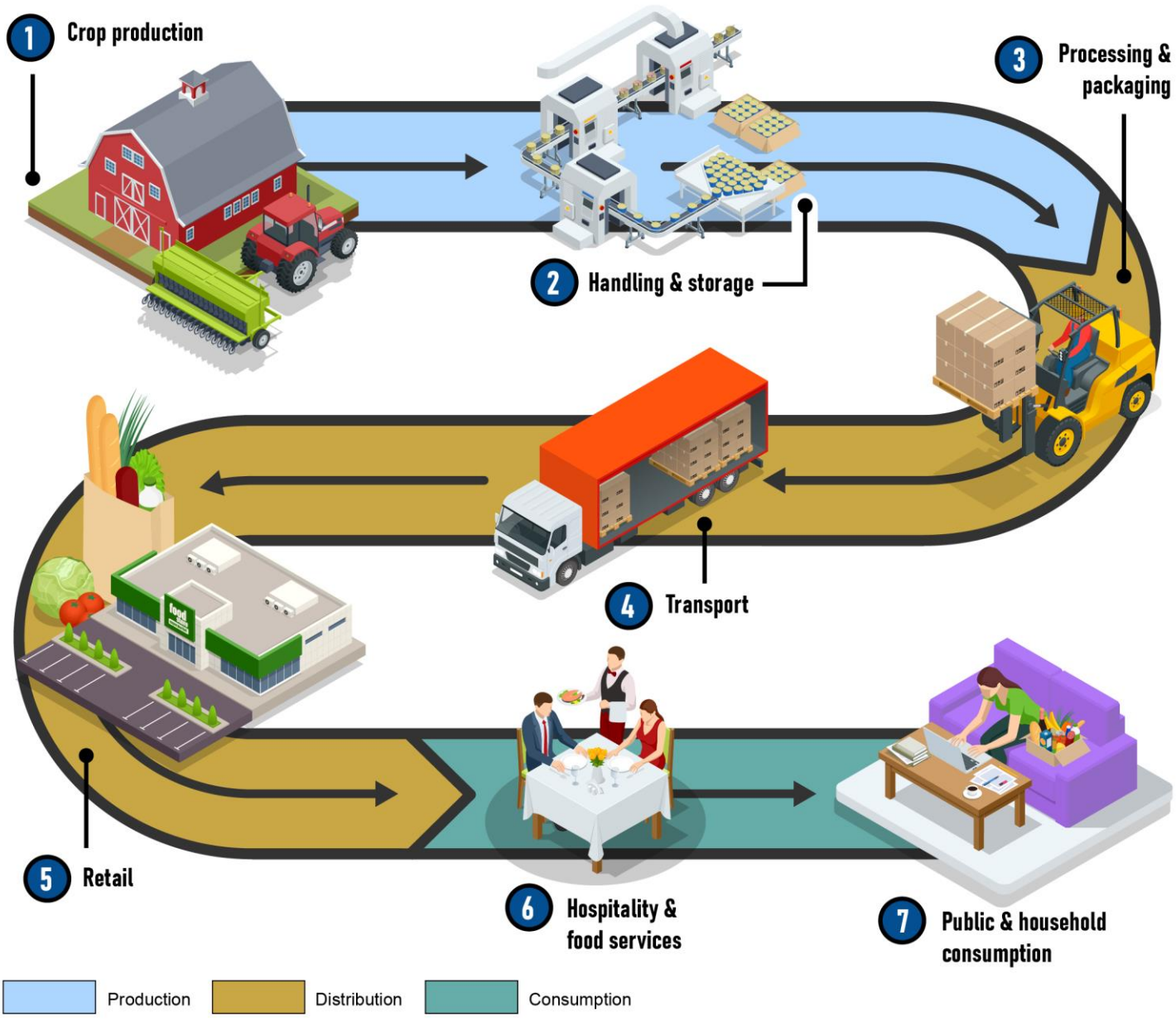
[12]We also contacted the American Farm Bureau, but the organization declined our request to participate.

the FA sector.[13] In 2024, USDA and FDA estimated that the sector is composed of an estimated 1.9 million farms, more than 220,000 registered facilities in food manufacturing, processing, and storage, and over 700,000 restaurants. According to USDA's Economic Research Service, agriculture, food, and related industries represented 5.5 percent of U.S. gross domestic product as of 2023, and agriculture and its related industries provided 10.4 percent of U.S. employment as of 2022. The FA sector includes the supply chains for feed, animals, and animal products; crop production; and the supply chains of seed, fertilizer, and other necessary related materials. It also includes the post-harvesting components of the food supply chain, from processing, production, and packaging through storage and distribution to retail sales, institutional food services, and restaurant or home consumption.[14] Figure 1 shows the various stages in the food supply chain.

[13]The other sectors are: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems.

[14]Department of Homeland Security, U.S. Department of Agriculture, and the Food and Drug Administration, *Food and Agriculture Sector-Specific Plan* (Washington, D.C.: 2015).

Figure 1. Stages in the Food Supply Chain



Sources: GAO analysis; Golden Sikorka/stock.adobe.com (illustrations). | GAO-27-108656

The FA sector has also become increasingly reliant on information and operational systems. Systems are needed for day-to-day food production facility operations, such as process control, supply tracking, and automated safety and security systems control. As we previously reported, satellite imagery, the global positioning system (GPS), and position, navigation, and timing technologies also support programs aimed at improving agricultural and ecological practices and allowing farmers and other producers to make better use of their land and resources.[15] In addition to improving food production, these operational systems support the transportation of agricultural and food products and processing and manufacture of food products.

We previously reported that within the FA sector, farmers and ranchers rely on what are known as precision agriculture technologies to manage crops or livestock.[16] These technologies are used to improve resource management through the precise application of inputs such as water, fertilizer, and feed, leading to more efficient agriculture production. However, as we discuss later in this report, this use of technology also creates cybersecurity vulnerabilities and the possibility of malicious acts committed by a threat actor. Figure 2 shows examples of precision agriculture technologies.

[15]GAO, *Precision Agriculture: Benefits and Challenges for Technology Adoption and Use*, GAO-24-105962 (Washington, D.C.: Jan. 31, 2024).

[16]GAO-24-105962.

Figure 2. Technologies Used in Precision Agriculture

Technology	Description
Auto-guidance	A guidance system that steers agricultural equipment with accuracy within centimeters. Newer equipment has this technology embedded, and add-on systems can be retrofitted on older equipment. Auto-guidance can provide for near-total automated steering while in the field. With auto-guidance, equipment can repeatedly drive along designated paths. Sometimes referred to as auto-steer.
Soil mapping	Soil mapping is used to identify soil properties at different locations. With a soil map, a farmer can decide on actions to prepare soil for growing agricultural commodities or on alternative land use options. To create a soil map, different technologies exist, including: • Soil sampling: measures soil factors including composition and nutrients. Though accurate, soil sampling can be expensive for large fields given the large number of samples required to generate an accurate soil map. • Electromagnetic sensing: measures the electrical characteristics of the soil, which reflect the soil's composition. • In situ sensors: can measure soil moisture.
Yield monitors and yield mapping	Yield monitors measure the harvest of a crop and tag the yield with a latitude and longitude coordinate. Data from yield monitors are used to create a yield map to quantify and characterize within-field production variability. Yield monitors are widely available for field crops, but they are not widely available for specialty crops. Other techniques such as overhead imagery can estimate crop yields for specialty crops.
Plant measurements	Plant characteristics can be measured by calculating vegetative indices using components of the electromagnetic spectrum. These indices provide estimates of characteristics, such as the amount of live green vegetation. Measurements are normally made remotely, with satellites, airplanes, or uncrewed aerial vehicles.
Variable rate technology	A system of sensors, controllers, and machinery that uses an application guidance map to direct the application of an input, such as herbicide or fertilizer, to a specific, identifiable location. Variable rate technology is dependent on measured farm data to build the application guidance map.
Farm management information systems (FMIS)	FMIS, a specific kind of software, is technology designed to assist farmers with performing data analysis from measured variability data, generate application guidance maps, and provide suggestions on specific farm operations, such as fertilization and irrigation scheduling to maximize yield and minimize costs. FMIS relies on data gathered by other precision agriculture technologies to make suggestions.

Sources: GAO review of literature and agency documentation (text); GAO (icons). | GAO-27-108656

The FA sector has many dependencies and relies on other critical infrastructures. These dependencies include the following sectors:

- **Water and Wastewater Systems Sector:** needed for clean irrigation and processed water.
- **Energy Sector:** powers equipment needed for agriculture production and food processing.
- **Communications Sector:** needed for satellite technologies, such as GPS; and public telecommunications systems for planting, harvesting, processing, and manufacturing of crops.
- **Chemical Sector:** provides fertilizers and pesticides used in the production of crops.
- **Transportation Systems Sector:** moves products and livestock.
- **Information Technology Sector:** needed for day-to-day food production facility operations, such as process control, supply tracking, and automated safety and security systems control.
- **Financial Services Sector:** serves as the financial backbone for food and agriculture business in the U.S.

A general disruption or cyberattack on these other sectors could disrupt food and agriculture operations, even if the FA sector was not the intended target. For example, a cyberattack on the water and wastewater systems sector could cause a water shortage and limit the ability of farmers to irrigate crops.

Sector Risk Management Agency Roles and Responsibilities

USDA and FDA. The nation's critical infrastructure is categorized into 16 sectors with at least one federal agency designated as the lead SRMA for each sector. SRMAs serve as the day-to-day federal interface for the prioritization and coordination of sector-specific risk management and resilience activities within their respective sectors. As specified in the Fiscal Year 2021 NDAA,[17] the co-SRMAs for the FA sector, USDA and HHS, acting through the FDA, are responsible for coordinating critical infrastructure protection efforts related to the physical security and cybersecurity of this sector. In addition, FDA and USDA share regulatory responsibility for food. According to its website, the FDA regulates about 77 percent of the U.S. food supply, including such things as bottled water,

[17]William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 9002, 134 Stat. 4765, 4768 (2021).

infant formulas, and food additives.[18] The USDA regulates meat, poultry, and egg products in accordance with the Federal Meat Inspection Act, Poultry Products Inspection Act, and Egg Products Inspection Act.

CISA. CISA is the lead federal agency for asset response and the national coordinator for the protection of critical infrastructure. As such, it is responsible for coordinating the overall federal effort to promote the security and resilience of critical infrastructure, among other things. In addition, CISA provides a variety of products and services to private and public sector organizations. These include training exercises, cybersecurity awareness webinars, network monitoring tools, risk assessment tools and services, and cyber threat alerts.

Federal Law and Policies Govern Sector Risk Management Agency Requirements

Federal law and policies establish roles and responsibilities for SRMAs to protect critical infrastructure, including the FA sector. Key law and policies include the Fiscal Year 2021 NDAA; the *National Security Memorandum on Strengthening the Security and Resilience of United States Food and Agriculture* (NSM-16);[19] and the *National Security Memorandum on Critical Infrastructure Security and Resilience* (NSM-22).[20]

Fiscal Year 2021 National Defense Authorization Act. The act updated the name for these agencies, stating that the term "sector risk management agency" holds the meaning previously given to the term "sector-specific agency."[21] The act also amended the Homeland Security Act of 2002 by adding a section on SRMAs and their responsibilities. See table 1 for the 16 SRMA requirements outlined in the Fiscal Year 2021 NDAA.

[18]Signed into law in 2011, the Food Safety Modernization Act gave the FDA new authorities to regulate the nation's food supply including mandatory recall authority and tasking the FDA with rulemaking and issuing guidance. FDA Food Safety Modernization Act, Pub. L. No. 111-353, 124 Stat. 3885 (2011).

[19]The White House, *National Security Memorandum on Strengthening the Security and Resilience of the United States Food and Agriculture* (NSM-16), 87 Fed. Reg. 69345 (Nov. 10, 2022).

[20]The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience* (NSM-22) (Apr. 30, 2024).

[21]6 U.S.C. § 652a.

Table 1. National Defense Authorization Act of 2021 Requirements for Sector Risk Management Agencies (SRMA)

Category of SRMA requirement	Description of requirement for responsible agencies
Sector coordination	Serve as a day-to-day federal interface for the prioritization and coordination of sector-specific activities and responsibilities under this title.
	Serve as the federal Government Coordinating Council chair for the designated sector or subsector.
	Participate in cross-sector coordinating councils, as appropriate.
Risk management	In coordination with the Director of the Cybersecurity and Infrastructure Security Agency (CISA), establish and carry out programs to assist critical infrastructure owners and operators within the designated sector or subsector in identifying, understanding, and mitigating threats, vulnerabilities, and risks to their systems or assets, or within a region, sector, or subsector.
	In coordination with the Director of CISA, recommend security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets.
Risk assessment	In coordination with the Director of CISA, identify, assess, and prioritize risks within the designated sector or subsector, considering physical security and cybersecurity threats, vulnerabilities, and consequences.
	In coordination with the Director of CISA, support national risk assessment efforts led by the Department of Homeland Security (DHS).
Information sharing	In coordination with the Director of CISA, facilitate the access to, and exchange of, information and intelligence necessary to strengthen the security of critical infrastructure, including through information sharing and analysis organizations and the National Cybersecurity and Communications Integration Center established pursuant to section 2209 of the act.
	Facilitate the identification of intelligence needs and priorities of critical infrastructure owners and operators in the designated sector or subsector, in coordination with the Director of National Intelligence and the heads of other federal departments and agencies, as appropriate.
	Provide the Director of CISA and facilitate awareness within the designated sector or subsector of ongoing, and where possible, real-time awareness of identified threats, vulnerabilities, mitigations, and other actions related to the security of the sector or subsector.
	Support the reporting requirements of DHS under applicable law by providing, on an annual basis, sector-specific critical infrastructure information.
Incident management	In coordination with the Director of CISA, support incident management and restoration efforts during or following a security incident.
	Support the Director of CISA, upon request, in national cybersecurity asset response activities for critical infrastructure.
Emergency preparedness	Coordinate with critical infrastructure owners and operators within the designated sector or subsector and the Director of CISA in the development of planning documents for coordinated action in the event of a national disaster, act of terrorism, or other man-made disaster or emergency.
	Participate in and, in coordination with the Director of CISA, conduct or facilitate, exercises and simulations of potential natural disasters, acts of terrorism, or other man-made disasters or emergencies within the designated sector or subsector.
	Support DHS and other federal departments or agencies in developing planning documents or conducting exercises or simulations when relevant to the designated sector or subsector.

Source: Summary of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. | GAO-27-108656

National Security Memorandum NSM-16. Issued in November 2022, NSM-16 includes responsibilities for federal agencies in the FA sector.[22] Specifically, the memorandum directs, among other things, DHS to coordinate with USDA and HHS to produce a comprehensive risk assessment for the FA sector that includes cyber threats, and review and update it on an annual basis.

National Security Memorandum NSM-22. Issued in April 2024, NSM-22 includes SRMA responsibilities that are to be implemented consistent with applicable law (including the Fiscal Year 2021 NDAA), presidential directives, and federal regulations.[23] These responsibilities include developing sector-specific risk assessments and risk management plans on a biennial basis.

Executive Order 14239, issued in March 2025, placed NSM-16 and NSM-22 under review.[24] According to Executive Order 14239, both memoranda were to be reviewed and recommended for revisions, recissions, and replacements within 180 days of the order. However, at the time of our review and as of September 2026, no modifications to the memoranda had been issued. Therefore, although they are under review, memoranda NSM-16 and NSM-22 outlining SRMA responsibilities are still valid, as the executive order did not explicitly rescind the NSMs.

The Food and Agriculture Sector Faces Increasing Cybersecurity Risks and Has Experienced Cyberattacks

Threat actors, such as state-sponsored hackers or criminal groups, are increasingly capable of carrying out cyberattacks on the FA sector. Increased use of technology to produce food and agriculture products has made the sector more vulnerable to cyberattacks. Although there are no official requirements to report incidents, a number of known cybersecurity incidents over the past 5 years have disrupted FA sector operations.

[22]The White House, *National Security Memorandum on Strengthening the Security and Resilience of the United States Food and Agriculture* (NSM-16), 87 Fed. Reg. 69345 (Nov. 10, 2022).

[23]The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience* (NSM-22) (Apr. 30, 2024).

[24]Exec. Order No. 14239, *Achieving Efficiency Through State and Local Preparedness*, 90 Fed. Reg. 13267 (Mar. 21, 2025).

Increased Use of Technology Has Heightened Cybersecurity Threats and Impacts in the Food and Agriculture Sector

The FA sector, like the other critical infrastructure sectors, faces increasing cybersecurity-related risks from a variety of threat actors, including criminal groups, hackers, insiders, nations, and terrorists (see table 2).

Table 2: Examples of Cybersecurity Threat Actors

Threat actor	Description of threat actor
Criminal groups	Criminal groups, including organized crime organizations, seek to use cyberattacks for monetary gain. Criminal groups often use ransomware—malicious software used to deny access to information technology systems or data—to hold systems or data hostage until a ransom is paid.
Hackers and hacktivists	Hackers break into networks for a challenge, revenge, stalking, or monetary gain, among other reasons. Hacktivists are ideologically motivated and use cyber exploits to further political goals such as free speech or to make a point.
Insiders	Insiders are entities (e.g., employees, contractors, vendors) with authorized access to an information system or enterprise who have the potential to cause harm through destruction, disclosure, modification of data, or denial of service. Such destruction can occur wittingly or unwittingly.
Nations	Nations, including nation-state, state-sponsored, and state-sanctioned groups, or programs, use cyber tools as part of their information-gathering and espionage activities. These groups can also possess the ability to launch cyberattacks that can cause disruptive effects to critical infrastructure.
Terrorists and domestic violent extremists	Terrorists and domestic violent extremists seek to destroy, incapacitate, or exploit critical infrastructure to threaten national security, inflict mass casualties, weaken the economy, and damage public morale and confidence.

Source: GAO analysis. | GAO-27-108656

The increased use of technologies to produce food and agriculture products has introduced new potential vulnerabilities into the sector that can be exploited if adequate controls have not been put into place. For example, failure to implement basic security measures, such as changing default passwords, can be exploited by threat actors. The threat actor could then manipulate data related to food quality, contamination testing, or traceability, potentially resulting in the distribution of unsafe or contaminated food products. This, in turn, can pose significant public health risks that could trigger product recalls and damage the reputation of food producers and suppliers. As another example, farmers use GPS-guided tractors and real-time soil sensors to improve efficiency, but these technologies can have cybersecurity vulnerabilities when connected to the internet. A cyberattack that takes advantage of these weaknesses, such as by compromising credentials, can then threaten production, leading to food supply chain disruptions. While not every disruption on a farm will lead to supply chain disruption, if a threat actor compromised

enough GPS-guided tractors and their data at the same time, it could potentially lead to a disruption of the food supply chain. Further, while small-scale attacks may only have limited impact, large-scale attacks or those targeting one or two key facilities could carry the potential for hunger and economic devastation across different geographical areas, spanning from local to international levels.

Cybersecurity attacks can also impact the processing of food and agriculture products in a way that may cause financial consequences to the victim company. For example, the Food and Ag-ISAC reported in 2024 that a ransomware attack could impact or disrupt processes along agriculture production lines, such as seed production. Any downtime because of an attack could then lead to a chain reaction of delays, potentially causing late planting or harvesting windows. This delay could require crops to be moved to other regions with an active growing season, which is typically only done in cases of severe weather conditions such as flooding.

Reported Cybersecurity Attacks in the Food and Agriculture Sector

Several cybersecurity incidents have been reported in the FA sector since 2021, of which ransomware appears to be the most common type. The Food and Ag-ISAC reported a total of 167 ransomware incidents in 2023, 206 in 2024, and 295 in 2025. In August 2026, the Food and Ag-ISAC also reported that 2026 is on pace to be one of the highest-volume ransomware years on record for the sector. It reported 227 ransomware incidents in the FA sector through July 2026. Most reported incidents aimed to shut down food production and distribution systems for ransom payments and spanned a broad spectrum of small and large companies, and farms. Cybersecurity incidents and supply chain disruption were among the greatest concerns to the FA sector, according to USDA, FDA, and DHS's 2024 draft sector risk assessment. However, FA sector owners and operators find it difficult to accurately characterize the likelihood of cybersecurity threats to a specific facility, making it difficult to prioritize security measures and prepare for potential cybersecurity incidents, according to USDA and FDA's 2024 draft risk management plan for the FA sector.[25] We discuss the status of the sector risk assessment and risk management plans in more detail below.

The actual number of cybersecurity incidents and impacts in the FA sector are not fully known beyond what is publicly reported on a voluntary

[25]U.S. Food and Drug Administration, and U.S. Department of Agriculture, *Food and Agriculture Sector Risk Management Plan* (forthcoming).

basis. As mentioned later in this report, USDA and FDA do not have any established voluntary methods for incident reporting and do not have authorities to require sector-wide reporting to them. Also, the Food and Ag-ISAC only knows what is voluntarily reported by its members or shared through its partners or open-source reporting. CISA also has a mechanism to voluntarily report cybersecurity incidents. See table 3 for examples of publicly reported cybersecurity attacks in the FA sector from 2021 to 2026, including the two most common types—ransomware and business email compromise—and the resulting impact on the victim company.

Table 3: Examples of Publicly Reported Cybersecurity Attacks in the Food and Agriculture Sector, 2021 to 2026

Date	Industry	Method of attack	Description of attack	Impact/financial loss
July 2026	Fairlife (Coca-Cola-owned dairy business)	Ransomware	Threat actors gained unauthorized access to a portion of Fairlife's systems, including its production-related systems.	The attack caused the company to halt production at its U.S. plants while Coca-Cola investigates.
April 2023	Israel's irrigation systems	Exploited vulnerabilities such as default passwords	Threat actors targeted water controllers for irrigation systems at farms in the Jordan Valley as well as wastewater treatment control systems of the Galil Sewage Corporation. Industrial control systems were hacked due to failure to implement basic security measures such as changing default passwords.	The attack caused damage to water controllers that manage field irrigation at a number of farms. Farmers were warned of the planned attack and some switched their irrigation systems from remote to manual. However, those who did not were impacted.
February 2023	Dole	Ransomware	Threat actors targeted half of Dole's legacy servers and one-quarter of its end-user computers. This led to unauthorized access to information and supply chain disruptions.	The attack disrupted Dole's operations, resulting in the temporary shutdown of production plants and the disruption of food supplies to U.S. grocery stores. The incident cost Dole $10.5 million.
August 2022	Multinational snack food and beverage company	Business email compromise	Threat actors sent a fake email order to a food distributor using the name of the distributor's chief financial officer, requesting two truckloads of powdered milk.	The attack caused the company to pay $160,000 to the supplier after fulfilling the fraudulent order.
May 2022	Worldwide manufacturer and distributor of farming equipment based in France (AGCO)	Ransomware	Threat actors targeted websites of a major provider of farming equipment in the U.S. with several ransomware attacks and data exfiltration.	The attack caused temporary shutdown of operations that lasted about two weeks, resulting in production losses, including a tractor assembly facility.
April 2022	Food manufacturer and supplier	Business email compromise	Threat actors impersonated a legitimate food company and sent the supplier a fraudulent web request for a bulk order of whole milk powder using the name of the supplier's president and nearly identical email address.	The attack caused the food manufacturer and supplier to lose $100,000 of whole milk powder.

Date	Industry	Method of attack	Description of attack	Impact/financial loss
March 2022	Multi-state grain company	Ransomware	Threat actors targeted a multi-state grain company, disrupting multiple services such as grain processing, seed, fertilizer, and logistics.	The attack caused disruptions in the company's grain processing service during critical preparation for the spring planting season.
February 2022	Food manufacturer	Business email compromise	Threat actors sent fraudulent email orders of milk powder and non-fat dry milk to a food manufacturer using real employee names and nearly identical email domains. The manufacturer believed the fraudulent orders were real and fulfilled the order for pickup before receiving full payment.	The attack caused the food manufacturer to lose $600,000 of whole milk powder and non-fat dry milk.
May 2021	Global meat processing company, JBS	Ransomware	Threat actors compromised JBS's computer networks, which forced the company to shut down some of the world's largest slaughterhouses in the U.S. and other countries.	The attack caused a temporary shutdown of meat processing plants, which caused a shortage in meat supply and a 25 percent spike in meat prices. JBS paid threat actors $11 million in bitcoin to regain access to its systems.
January 2021	U.S. farm	Ransomware	Threat actors targeted the farm's internal servers by gaining administrator-level access through compromised credentials.	The attack caused a $9 million production loss due to a temporary shutdown of farming operations.

Source: GAO analysis of publicly available data. | GAO-27-108656

USDA and FDA Actions Met Most Cyber-Related Aspects of SRMA Requirements, But Key Steps Remain

As previously mentioned, the Fiscal Year 2021 NDAA establishes 16 requirements for each of the SRMAs to address risks, including cybersecurity-related risks, in coordination with CISA. The requirements fall under these six categories: sector coordination, risk management, risk assessment, information sharing, incident management, and emergency preparedness.

While USDA and FDA have taken steps to meet most of the cybersecurity-related aspects of the requirements, they have not met all of them, as shown in table 4. Detailed information on the status of these requirements follows the table.

Table 4. Extent to Which Sector Risk Management Agencies (SRMA) Have Met Requirements for Food and Agriculture Sector Cybersecurity

Category of requirement	Description of requirement	Assessment[a]	
		USDA	FDA
Sector coordination	Serve as a day-to-day federal interface for the prioritization and coordination of sector-specific activities and responsibilities under this title.	Met	Met
	Serve as the federal Government Coordinating Council chair for the designated sector.	Met	Met

Category of requirement	Description of requirement	Assessment[a]	
		USDA	FDA
	Participate in cross-sector coordinating councils, as appropriate.	Met	Met
Risk management	In coordination with the Director of the Cybersecurity and Infrastructure Security Agency (CISA), establish and carry out programs to assist critical infrastructure owners and operators within the designated sector in identifying and mitigating threats and risks to their systems or assets.	Met	Met
	In coordination with the Director of CISA, recommend security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets.	Met	Met
Risk assessment	In coordination with the Director of CISA, identify, assess, and prioritize risks within the designated sector considering physical security and cybersecurity threats, vulnerabilities, and consequences.	Met	Met
	In coordination with the Director of CISA, support national risk assessment efforts led by the Department of Homeland Security (DHS).	Met	Met
Information sharing	In coordination with the Director of CISA, facilitate exchange of information and intelligence necessary to strengthen the security of critical infrastructure, including through information sharing and analysis organizations and the National Cybersecurity and Communications Integration Center.	Met	Met
	Facilitate the identification of intelligence needs and priorities of critical infrastructure owners and operators in the designated sector, in coordination with the Director of National Intelligence and the heads of other federal departments and agencies.	Met	Met
	Provide the Director of CISA—and facilitate real-time awareness of—ongoing threats, vulnerabilities, mitigations, and other actions related to the security of the sector.	Partially met	Partially met
	Support the reporting requirements of DHS under applicable law by providing sector-specific critical infrastructure information on an annual basis.	Met	Met
Incident management	In coordination with the Director of CISA, support incident management and restoration efforts during or following a security incident.	Met	Met
	Support the Director of CISA, upon request, in national cybersecurity asset response activities for critical infrastructure.	Met	Met
Emergency preparedness	Coordinate with critical infrastructure owners and operators within the designated sector, and the Director of CISA, in developing plans for coordinated action in the event of a national disaster, act of terrorism, or other man-made disaster or emergency.	Met	Not met
	Participate in and, in coordination with the Director of CISA, conduct or facilitate exercises and simulations of potential natural disasters, acts of terrorism, or other man-made disasters or emergencies within the designated sector.	Partially met	Partially met
	Support DHS and other federal departments or agencies in developing planning documents or conducting exercises or simulations when relevant to the designated sector.	Not applicable[b]	Not applicable[b]

Sources: GAO analysis of Fiscal Year 2021 National Defense Authorization Act; and U.S. Department of Agriculture (USDA) and Food and Drug Administration (FDA) data. | GAO-27-108656

[a]We assessed the SRMAs' actions to address cyber-related aspects of each category of requirement.

[b]This requirement was not applicable because the agencies did not receive any requests for support, according to agency officials.

Sector Coordination. USDA and FDA met the three sector coordination requirements:

- The agencies met the requirement to serve as day-to-day federal interfaces for the prioritization and coordination of sector activities and responsibilities by facilitating joint sector membership meetings where cybersecurity is discussed. USDA officials stated that they also coordinate with FDA and CISA through conference calls and email. According to FDA officials, FDA works closely with CISA and directs individuals to CISA for incidents. The agencies also work with CISA to develop cybersecurity resources (e.g., fact sheets, alerts, and advisories) for the FA sector. In addition, the FDA webpage includes various CISA cybersecurity resources.
- The co-SRMAs also met the requirement to serve as federal Government Coordinating Council chairs for the sector.
- USDA and FDA further met the requirement to participate in cross-sector coordinating councils. Both agencies are members of the Federal Senior Leadership Council, which serves as the primary cross-sector council for SRMAs and other agencies with responsibility for critical infrastructure security and resilience.

Risk Management. USDA and FDA met the two risk management requirements:

- The agencies met the requirement to establish and carry out programs to assist sector owners and operators in identifying and mitigating threats to their systems or assets. According to USDA officials, USDA submitted a draft *Food and Agriculture Sector Risk Management Plan* to the National Security Council and CISA in early January 2025.[26] The draft plan aligns risk management with sector goals, identifies cybersecurity risks and threats to the sector, and includes measures of progress. USDA officials told us that it has not received any comments or feedback since submitting the plan due to Executive Order 14239 ordering the review of the memoranda, as discussed above. Therefore, the plan is not considered final pending the National Security Council and CISA's review.
- The co-SRMAs also met the requirement to recommend security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets. The draft *Food and Agriculture*

[26]U.S. Food and Drug Administration, and U.S. Department of Agriculture, *Food and Agriculture Sector Risk Management Plan* (forthcoming).

Sector Risk Management Plan includes cybersecurity mitigations for the sector. Although the sector risk management plan has not been finalized, USDA and FDA have demonstrated other ways in which they recommend security measures to the sector. For example, in March 2023, the co-SRMAs released the *120-Day Food and Agriculture Interim Risk Review*.[27] The interim risk review included several activities to mitigate cybersecurity risks, such as prioritizing information sharing about cyberattacks, researching cybertheft of FA intellectual property, and encrypting information transfers. In addition, in June 2026, USDA coordinated with CISA to issue a cybersecurity advisory regarding mitigations for automatic tank gauge attacks.[28]

Risk Assessment. USDA and FDA met the two risk assessment requirements:

- The agencies met the requirement to identify, assess, and prioritize risks within the sector, with consideration to cybersecurity threats, vulnerabilities, and consequences. For example, the *120-Day Food and Agriculture Interim Risk Review* identified risks to the sector, such as risks associated with automation, precision farming, and digital agriculture. The co-SRMAs also developed an assessment of potential artificial intelligence risks in the sector. In addition, USDA, FDA, and DHS drafted the *Sector-Specific Risk Assessment 2024,*[29] which was developed in response to requirements in NSM-16 and NSM-22. The draft assessment includes several cybersecurity scenarios that assess risks to the sector. As previously mentioned, the risk assessment has not been reviewed and finalized because the memoranda are under review.

[27]Department of Health and Human Services, U.S. Department of Agriculture, and Department of Homeland Security, *National Security Memorandum on Strengthening the Security and Resilience of United States Food and Agriculture: 120-Day Food and Agriculture Interim Risk Review*.

[28]According to the cybersecurity advisory, automatic tank gauge systems are widely used in the FA sector for automated and remote monitoring of storage tank parameters, including fuel and liquid levels, temperature, and possible leak detection. Cybersecurity and Infrastructure Security Agency et al., *CISA and Partners Urge Hardening Automatic Tank Gauge Systems* (Washington, D.C.: June 2, 2026).

[29]U.S. Department of Agriculture, U.S. Food and Drug Administration, and U.S. Department of Homeland Security, *Sector-Specific Risk Assessment 2024: Food and Agriculture* (Washington, D.C.: forthcoming). The forthcoming risk assessment was completed and submitted to the National Security Council and CISA in January 2025. However, according to USDA and FDA officials, the risk assessment has not been reviewed and finalized due to the pause of NSM-22 by Executive Order 14239.

- The agencies also met the requirement to support national risk assessment efforts led by DHS. For example, in addition to releasing the *120-Day Food and Agriculture Interim Risk Review* alongside USDA, FDA officials stated that the agency provides FA sector vulnerability information to DHS's Probabilistic Analysis for National Threats Hazards and Risks program.[30] According to FDA officials, the agency provided this input verbally to the program during in-person meetings. The *Sector-Specific Risk Assessment 2024* also supports DHS's national risk assessment efforts.

Information Sharing. USDA and FDA met three of the four information sharing requirements and partially met one of the requirements:

- The agencies met the requirement to facilitate access to and exchange of information necessary to strengthen the cybersecurity of the sector. As mentioned earlier, USDA and FDA facilitate cybersecurity information sharing through joint sector meetings. USDA also shared information with the sector through biweekly sector communication emails and targeted communications. For example, in February 2026, USDA sent an email to sector membership that included cybersecurity alerts and advisories from January to February. In addition, FDA shared cybersecurity resources through its website, and the co-SRMAs developed joint cybersecurity advisories. For example, in December 2022, USDA and FDA co-authored an advisory on how criminals compromise business emails to steal shipments of food products and ingredients valued at hundreds of thousands of dollars.
- USDA and FDA also met the requirement to facilitate the identification of intelligence needs and priorities of the sector. The agencies coordinated with representatives from organizations within the FA sector to share key sector intelligence information with CISA. The representatives from the Food and Agriculture Sector Coordinating Council are also included in FA sector intelligence briefings provided by USDA. According to USDA and FDA officials, if they receive any cybersecurity-related information from the sector, they share it with DHS's CISA.
- The co-SRMAs partially met the requirement to provide CISA with—and facilitate awareness within the sector of—information on ongoing

[30]DHS's Probabilistic Analysis for National Threats Hazards and Risks program was established to provide critical technical information on chemical, biological, radiological, and nuclear hazards, to enable better informed decisions for defense against threats from weapons of mass destruction.

and real-time threats, vulnerabilities, mitigations, and other actions related to the security of the sector. To facilitate cybersecurity awareness within the sector, the co-SRMAs and CISA work together to develop toolkits and cobranded cybersecurity factsheets for the sector. According to USDA officials, the agency also provides CISA with threat and mitigation information as it becomes available. For example, in May 2026, USDA provided input for CISA's June 2026 advisory on automatic tank gauge attacks and informed CISA of the widespread use of automatic tank gauges in agricultural facilities. In addition, FDA officials stated that CISA's liaison to the sector participates in meetings and information exchanges with sector membership.

However, the co-SRMAs do not provide CISA with continuous real-time awareness of threats, vulnerabilities, mitigations, and other actions related to the cybersecurity of the sector. In addition, FDA officials stated that FDA does not have a structured mechanism for continuously collecting cybersecurity data, and the agency also does not track the usage of cybersecurity resources in the sector. Therefore, it is unclear how the co-SRMAs would receive and be able to provide CISA with real-time cybersecurity threat or vulnerability information.

- The co-SRMAs met the requirement to support the reporting requirements of DHS by providing sector-specific information on an annual basis. USDA provided CISA with information for USDA's collaboration on the automatic tank gauge advisory, as well as in response to requests for sector information after major cyber incidents. FDA also provides information to DHS's Probabilistic Analysis for National Threats Hazards and Risks program. As mentioned earlier, the draft sector-specific risk assessment was developed in response to NSM-16, which requires DHS to work with the co-SRMAs to develop annual risk assessments for the sector.

Incident Management. USDA and FDA met the two incident management requirements:

- The co-SRMAs met the requirement to support incident management and restoration efforts during or following security incidents. For example, on behalf of the co-SRMAs, USDA officials responded to CISA's July 2024 request for information on sector impacts following a global IT outage. USDA also responded to the Federal Bureau of Investigation's March 2026 notification of a ransomware attack on a food store.

- The agencies also met the requirement to support CISA, upon request, in national cybersecurity asset response activities for critical infrastructure. As mentioned above, the co-SRMAs communicate with CISA in response to requests for information from CISA, following reported cyber incidents.

Emergency Preparedness. USDA met one of the emergency preparedness requirements, partially met one requirement, and the third requirement was not applicable. FDA partially met one of the three requirements, did not meet one requirement, and the third requirement was not applicable:

- USDA met the requirement to coordinate with sector owners and operators and CISA in developing planning documents for coordinated action in the event of a cyber incident. USDA offers a food defense exercise package to facilities the agency regulates, which includes a ransomware scenario. USDA also drafted a cybersecurity situational report template in late fiscal year 2024 that could be used to communicate with sector partners for sector impacting events, such as the CrowdStrike-related IT outages in July 2024.[31] However, procedures and policies to implement the template were put on hold after the change in administration, and USDA does not have any plans to finalize the template unless there is a request from CISA. FDA did not meet this requirement. The FDA webpage on food-related emergency exercise scenarios did not include a cybersecurity scenario. Such a food-related cyber scenario would have fulfilled FDA's requirement for providing emergency preparedness planning documents in the event that a cyberattack impacted companies under FDA's regulatory responsibilities. According to FDA officials, the agency has not developed or published a complete exercise scenario focused specifically on a cyber-related food emergency.
- USDA and FDA partially met the requirement to participate in an exercise and simulation of potential cyber incidents within the FA sector. The co-SRMAs participated in CISA's Cyber Storm IX exercise in 2024, where participants, including 30 attendees from the FA sector, exercised incident response, information sharing, and coordination in response to a simulated cyber campaign against

[31]In July 2024, a software update from the cybersecurity firm CrowdStrike caused Microsoft Windows operating systems to crash—resulting in potentially one of the largest IT outages in history. The outage disrupted critical infrastructure operations by grounding commercial flights and interrupting critical hospital care, among other impacts.

critical infrastructure. The FA sector served as the primary impacted sector for the exercise. However, the co-SRMAs have not conducted or facilitated exercises and simulations of cyber incidents in the sector. USDA officials stated that USDA is not planning additional exercises based on the results of Cyber Storm IX, and FDA officials stated that FDA is not currently leading any emergency preparedness exercises related to cybersecurity in the FA sector.

- The requirement to support DHS and other federal departments or agencies in developing cybersecurity planning documents or conducting cybersecurity exercises or simulations was not applicable. According to USDA and FDA officials, the co-SRMAs did not receive any related requests. The officials stated that they were not aware of any requests to support DHS or other agencies in their efforts.

Several factors contributed to the SRMAs' partially or not meeting the five cybersecurity requirements in the categories of information sharing and emergency preparedness. These include a lack of resources and staffing, according to agency officials, and limitations on tracking and reporting cyber incidents.

- According to USDA officials, USDA's Office of Homeland Security has no full-time equivalents and it does not receive appropriations for its SRMA responsibilities. The officials also stated that USDA has limited to no expertise about private sector cybersecurity operations or the cybersecurity-related challenges that the private sector faces. In addition, according to USDA officials, USDA has no authority to require the private sector to implement cybersecurity mitigations, so the agency is focused on promoting cyber awareness. Further, USDA has no resources for analysis of any cybersecurity threats, vulnerabilities, or consequences. Also, according to officials, the agency has limited expertise and no resources for addressing cyber incidents in the FA sector beyond those used to protect USDA's own network.
- According to an FDA official, the agency has no dedicated funding to fulfill its cyber-related SRMA responsibilities. In addition, FDA officials stated that FDA does not have a structured mechanism for collecting cybersecurity data in the sector.
- Although the agencies met the incident management requirements, officials noted that their efforts were constrained by a limited ability to track and report cyber threats. USDA stated that its role is limited due to lack of specialized expertise and lack of authorities to require sector-wide reporting. In addition, FDA does not have a reporting

mechanism for food and agriculture organizations in the sector to report cyber incidents to FDA. FDA queried its Reportable Food Registry program and it did not find any cyber-related incidents for the past five years.[32] According to FDA officials, if a cybersecurity incident resulting in food contamination or adulteration does not have adverse health consequences for humans or animals, the incident does not meet reporting requirements and would not be captured by the registry. Further, although the FDA webpage states that FDA's Office of Criminal Investigations is capable of conducting investigations of cybercrimes, an FDA official told us that the agency does not track cyber incidents.

While USDA and FDA have met most of the SRMA requirements, they both reported having limited resources to address critical cybersecurity activities, such as information sharing and cybersecurity emergency preparedness activities. Until USDA and FDA have assessed whether they can reprioritize their resources and staffing, or if they need additional resources to provide more support to meet the SRMA requirements, the FA sector will be more vulnerable to cybersecurity risks and attacks, potentially disrupting the nation's food and agriculture supply chains and resulting in significant economic and environmental impact.

Selected Private Sector Organizations Described Actions and Views to Improve FA Sector Cybersecurity

Officials we spoke with from six private sector organizations that comprise a cross section of the FA sector, such as trade associations in the grain, dairy, and meat industries, described actions taken to collaborate with their members to share cybersecurity resources, threat alerts, and best practices, as well as efforts to collaborate with federal agencies. They also reported challenges associated with addressing threats to the FA sector and suggested ways to improve the cybersecurity of the sector.

Selected Private Sector Organizations Reported Efforts to Improve Sector Cybersecurity

Officials from the six private sector organizations included in our review reported multiple actions to improve the cybersecurity of the FA sector. According to a Food and Ag-ISAC official, the organization shares customized threat intelligence with its members based on its analysis, including weekly reports summarizing key threats and vulnerabilities that were observed as either impacting or being relevant to the FA sector. In

[32]According to FDA officials, the Reportable Food Registry program captures information about adulterated food that poses health risks, regardless of how the adulteration occurred (i.e., through traditional contamination, intentional adulteration, process failures, or cybersecurity incidents).

addition, it shares information and alerts issued by the IT Information Sharing and Analysis Center (IT-ISAC)[33] and CISA. Although the alerts are not always specific to the FA sector, the official stated that the alerts provide insight for its members. For example, the Food and Ag-ISAC received CISA's document *Adapting Zero Trust Principles to Operational Technology* as a public release and shared it with its members.[34] It also leverages a threat intelligence platform to track over 230 threat actors.

The ISAC further partners with different universities (i.e., the University of Iowa, the University of Nebraska, and Virginia Tech, among others) with agricultural extensions to distribute cybersecurity guidance and provides threat summaries to both members and non-member association and industry partners.[35] The Food and Ag-ISAC also participates in virtual calls, webinars, conferences and speaking opportunities with its partner organizations.

Officials from the five other private sector organizations also told us about efforts to collaborate on cybersecurity with their members. For example:

- One organization provides input to its members on cybersecurity policy. In addition, this organization works with federal agencies to obtain appropriate security clearances for its members so that they can receive and provide feedback on sensitive cybersecurity-related information related to the sector.
- One organization's webpage connects members with cybersecurity resources, such as the Food and Ag-ISAC's *Cybersecurity Guide for Small and Medium-Sized Businesses*. In addition, officials from this organization have communicated with the Center for Internet Security[36] to break down the National Institute of Standards and

[33]The IT-ISAC is the source for security information impacting the information technology sector. The IT-ISAC is recognized by DHS and the Information Technology Sector Coordinating Council as the sector's designated information-sharing forum.

[34]Cybersecurity and Infrastructure Security Agency, *Adapting Zero Trust Principles to Operational Technology* (Washington, D.C.: Apr. 29, 2026).

[35]Cooperative Extensions is a nationwide partnership between federal government (USDA), state land-grant universities, and local governments that delivers research-based knowledge to the public.

[36]The Center for Internet Security, Inc. is a nonprofit organization whose stated mission is to make the connected world a safer place for people, businesses, and governments through collaboration and innovation and providing products and services to proactively safeguard against emerging threats.

Technology (NIST) Cybersecurity Framework 2.0 for their members to more easily implement.[37]

- Another organization's cybersecurity working group created a set of best practices that included ways to implement NIST cybersecurity standards. The organization's cybersecurity working group also helped to start the Food and Ag-ISAC, which its members have joined, and which is valuable, according to an official. Lastly, members of the organization shared descriptions of incidents and the consequences of cyber-related incidents—such as the impact of having to do payroll by hand when a system was down—through a private listserv. Members impacted by cyber-related incidents also shared mitigation strategies, such as the need to print out cyber insurance policies so the information is available in hard copy when systems are down.
- Two organizations worked to provide education or awareness training among their members by collaborating with other organizations to develop their education programs and create cybersecurity sessions for an event.
- One organization disseminates DHS and CISA guidance and best practices to its members.

In addition, officials from the organizations told us that they and their members collaborate with federal agencies in a number of ways. For example, one organization facilitates members reporting cybersecurity incidents to the Federal Bureau of Investigation, U.S. Secret Service, and DHS/Homeland Security Investigations. Another organization works with the U.S. Coast Guard's Alternative Security Program to develop cybersecurity requirements for member companies that operate in the ports.[38] In addition, a Food and Ag-ISAC official stated that they collaborate with USDA and FDA to identify coordination gaps and

[37]The NIST Cybersecurity Framework 2.0 provides guidance to industry, government agencies and other organizations to manage cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization—regardless of its size, sector, or maturity—to better understand, assess, prioritize, and communicate its cybersecurity efforts. National Institute of Standards and Technology, *The NIST Cybersecurity Framework 2.0* (Gaithersburg, MD: Feb. 26, 2024).

[38]Alternative Security Programs give groups of similar vessels and/or facilities an alternative way to comply with the Maritime Transportation Security Act, which directs the U.S. Department of Transportation to develop security measures for domestic maritime facilities and the vessels that use them.

determine how agencies and industry can work together more effectively to coordinate cybersecurity-related efforts to the FA sector.

Selected Private Sector Organizations Identified Challenges to Improving Sector Cybersecurity

In addition to describing actions to improve sector cybersecurity, the six selected private sector organizations that we interviewed reported multiple challenges and opportunities to improve cybersecurity, including:

Diminished federal and private sector coordination. Organizations described a general lack of coordination and information sharing on the part of federal agencies responsible for sector cybersecurity. For example, officials from two organizations stated that the termination of a key forum for communication—the Critical Infrastructure Partnership Advisory Council (CIPAC)— had stifled communications between the private sector and the federal government when it comes to sharing information.[39] They added that, as a result, the relationship between the sector and the government has been negatively impacted.[40] Federal officials expressed similar concerns, with USDA officials stating that the termination of CIPAC had negatively impacted cybersecurity communications at joint sector meetings. CISA officials also stated that CIPAC established a valuable forum for critical infrastructure partners to provide consensus advice to the federal government, but without its legal protections to shield executives from antitrust laws, the industry may be reluctant to openly share information with the federal government.

In July 2026, DHS announced the Alliance of National Councils for Homeland Operational Resilience-Critical Infrastructure, referred to as ANCHOR-CI, to replace CIPAC by providing forums in which government officials can engage with private sector entities to review the current threat environment, discuss potential vulnerabilities, and form recommendations on securing critical infrastructure and cyberspace. However, according to CISA officials, ANCHOR-CI is in the formative stages and had not held any meetings at the time of our review.

[39]In accordance with Executive Order 14217, *Commencing the Reduction of the Federal Bureaucracy,* the Secretary of Homeland Security determined that the termination of CIPAC, among other discretionary Federal Advisory Committees, was in the best interest of DHS. Department of Homeland Security, *Notice of Termination of Discretionary Federal Advisory Committees* (Washington D.C.: Mar. 13, 2025).

[40]DHS established CIPAC to facilitate interaction between governmental entities and representatives from the community of critical infrastructure owners and operators. Its membership was comprised of government and sector coordinating councils. As of 2025, CIPAC has been terminated.

Lack of dedicated cybersecurity staff internal to food and agriculture organizations. Organizations described challenges having internal staff with cybersecurity expertise. Officials from one organization that comprised a segment of the FA sector stated that many companies do not have the necessary technical expertise, so they rely on a third party for cybersecurity needs, such as for incident response and threat intelligence.

Loss of knowledgeable federal staff. Organizations reported that employee turnover and general attrition of staff in key federal agency cybersecurity roles, such as at CISA, had resulted in challenges. For example, an official from one organization stated that they had pointed members with less cybersecurity maturity to CISA for assistance. However, the official stated that their contacts at CISA had either been furloughed or left the agency, so they had stopped sending members to CISA for assistance.

Rise of artificial intelligence. Organizations reported uncertainties associated with the speed and scale of emerging artificial intelligence technology. For example, a Food and Ag-ISAC official stated that artificial intelligence is identifying vulnerabilities at machine scale, while their processes for mitigating them operate at human speed. Another organization stated that artificial intelligence has been a challenge for them and has been a topic at recent industry conferences.

Selected Private Sector Organizations Identified Potential Opportunities to Improve Sector Cybersecurity

The six organizations suggested ways to improve the cybersecurity of the sector. Officials from four organizations stated that:

- It is critical to replace CIPAC to maintain relationships between USDA and CISA and the organization's members. As previously noted, in July 2026, DHS announced that ANCHOR-CI would replace CIPAC, but according to CISA officials, ANCHOR-CI is still in its formative stages.
- The Cybersecurity Information Sharing Act of 2015 needs a long-term extension of its protections to ensure continued threat intelligence sharing within the industry and between industry and government.[41]

[41]The Cybersecurity Information Sharing Act of 2015 offered information protection measures, antitrust protections, liability protections, and protections from disclosure (e.g., in court proceedings) that are explicit and specific to the act. The act's provisions were due to expire on September 30, 2026; however, they were extended to December 11, 2026, via the Continuing Appropriations and Extensions Act, 2027. Pub. L. No. 119-103 (Sept. 2, 2026).

- A single reporting structure for cybersecurity incidents would be beneficial. There are currently multiple reporting structures that private sector organizations can use to report cybersecurity incidents, including in the FA sector. For example, private sector organizations may report to the Federal Bureau of Investigation, CISA, USDA's Office of Homeland Security, the U.S. Secret Service, and DHS's Homeland Security Investigations.
- Free cybersecurity assessments would help companies become more aware of their cybersecurity posture within the sector. According to CISA officials, CISA offers a number of no cost cybersecurity tools and services to help organizations build and maintain a robust and resilient cyber framework.

Conclusions

The FA sector faces increased cybersecurity threats and past incidents have resulted in millions of dollars in lost revenue and disruptions to the nation's food supply chain. These threats are amplified by the sector's increasing use of internet-connected technologies in the production, harvesting, and storing of food. When poorly secured, these technologies can be used to illicitly access systems and launch ransomware or supply chain disruption attacks. Further, the sector's critical dependencies with multiple other infrastructure sectors underscores the importance of ensuring that food and agriculture-related equipment is as secure as possible.

To respond to threats such as these, USDA and FDA have taken steps to improve FA sector cybersecurity in accordance with their responsibilities as the sector's co-SRMAs. While USDA and FDA have met most of the SRMA requirements, they both reported having limited resources to address critical cybersecurity activities, such as information sharing and cybersecurity emergency preparedness activities. Until USDA and FDA have assessed whether they can reprioritize their resources and staffing, or if they need additional resources to provide more support to meet the SRMA requirements, the FA sector will be more vulnerable to cybersecurity risks and attacks, potentially disrupting the nation's food and agriculture supply chains and resulting in significant economic and environmental impact.

Recommendations for Executive Action

We are making five recommendations, two to the Department of Agriculture and three to the Department of Health and Human Services:

- The Secretary of Agriculture should ensure that the Director of the Office of Homeland Security fully implements the SRMA requirement related to information sharing of cybersecurity threats and

vulnerabilities with CISA, including by assessing whether resources should be reprioritized or requested to continuously collect information on cybersecurity threats. (Recommendation 1)

- The Secretary of Agriculture should ensure that the Director of the Office of Homeland Security fully implements the SRMA requirement related to facilitating or conducting cybersecurity emergency preparedness exercises and simulations, including by assessing whether resources should be reprioritized or requested to do so. (Recommendation 2)
- The Secretary of Health and Human Services should ensure that the Director of the Food and Drug Administration's Office of Coordinated Outbreak Response fully implements the SRMA requirement related to information sharing of cybersecurity threats and vulnerabilities with CISA, including by assessing whether resources should be reprioritized or requested to continuously collect information on cybersecurity threats. (Recommendation 3)
- The Secretary of Health and Human Services should ensure that the Director of the Food and Drug Administration's Office of Coordinated Outbreak Response fully implements the SRMA requirement related to facilitating or conducting cybersecurity emergency preparedness exercises and simulations, including by assessing whether resources should be reprioritized or requested to do so. (Recommendation 4)
- The Secretary of Health and Human Services should ensure that the Director of the Food and Drug Administration's Office of Coordinated Outbreak Response fully implements the SRMA requirement related to developing planning documents for coordinated action in the event of cybersecurity disasters or emergencies. (Recommendation 5)

Agency Comments and Our Evaluation

We provided a draft of this report to the USDA, HHS, and DHS for review and comment. Of the two agencies to which we made recommendations (HHS and USDA), HHS agreed with all three recommendations and USDA disagreed with its two recommendations and requested us to remove or redirect the recommendations. DHS had no comments on the draft. In addition, USDA and HHS provided technical comments, which we have incorporated, as appropriate.

In written comments, reproduced in appendix I, HHS agreed with all three recommendations and described actions FDA is taking in response to the recommendations:

- Regarding recommendation 3 on the information sharing requirement, FDA stated that it is reviewing the flow of information received from CISA and the Federal Bureau of Investigation and considering cybersecurity monitoring processes and related analyses.

- In response to recommendation 4 related to facilitating and conducting cybersecurity emergency preparedness exercises, FDA stated that it is considering a portfolio of potential work to include both cybersecurity planning documents and preparedness exercises. In addition, FDA noted ongoing willingness to participate in interdepartmental cybersecurity exercises and simulations.

- Regarding recommendation 5 related to developing planning documents for coordinated action in the event of cybersecurity disasters or emergencies, FDA stated that it is initiating plans to meet this recommendation and considering adding finalized scenarios to the FDA webpage on food-related emergency exercise scenarios.

In comments provided via email, an Associate Director from USDA's Office of Homeland Security requested that we remove the two recommendations or direct the recommendations to USDA's Chief Information Officer.

- Specifically, the official stated that the department's Office of Homeland Security lacked the funding, authorities, and subject matter expertise to fulfill the currently unmet SRMA requirements. The USDA official further stated that the department's Chief Information Officer was responsible for coordinating USDA network threat reporting and cybersecurity operations. However, USDA's Office of Homeland Security is the designated SRMA office responsible for carrying out SRMA programs, projects, activities, and fulfilling NDAA requirements. In this capacity, the office is responsible for fulfilling the department's SRMA responsibilities as established by law, including addressing cybersecurity-related risks faced by private sector organizations in the FA sector. As such, we maintain that our recommendations are appropriately directed to the responsible USDA office.

- With regard to recommendation 1, the official stated that USDA is in compliance with the NDAA information sharing requirement and said that the law requires SRMAs to provide, “where possible,” real-time information on identified threats, vulnerabilities, mitigations, and related actions. However, the NDAA also requires that SRMAs facilitate awareness of ongoing threats and other actions to CISA and the designated sector or subsector. Our recommendation is specific to facilitating awareness of ongoing threats, and, additionally, recommends that USDA should assess whether resources should be reprioritized to continuously collect information on cyber threats. As acknowledged by USDA’s response to our report, the department only provides CISA with threat and mitigation information as it becomes available. As a result, we maintain this recommendation is appropriate.

- Concerning recommendation 2, the official stated that the NDAA does not require cybersecurity exercises but directs SRMAs to conduct or facilitate exercises and simulations of potential natural disasters, acts of terrorism, or other man-made disasters or emergencies within the designated sector or subsector. However, the NDAA explicitly recognizes that cyber-related threats are an aspect of critical infrastructure protection. A cyberattack can be a terrorist act or a man-made disaster, so exercises should be developed to better prepare the sector for cyber threats. As previously mentioned, and to the department’s credit, USDA participated in CISA’s Cyber Storm IX exercise in 2024, where attendees from the FA sector exercised potential cyber incidents within the sector. However, as our report notes, USDA officials told us that there were no plans for further cyber exercise and simulation in the sector. In addition, the USDA official stated in the emailed response to our draft report that the department’s Chief Information Officer has an active exercise program for USDA systems and applications. However, the exercise program is for USDA’s internal systems and is not based on potential cyber incidents faced by organizations in the FA sector. Our recommendation is specific to cyber exercises and simulations within the FA sector, and additionally, recommends that USDA should assess whether resources should be reprioritized to conduct cyber exercises and simulations. As a result, we maintain that this recommendation is appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretaries of Agriculture, Health and Human Services, and Homeland Security, the Acting Commissioner of the Food and Drug Administration, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at HinchmanD@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.

//SIGNED//

David B. Hinchman
Director, Information Technology and Cybersecurity

Appendix I: Comments from the Department of Heath and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

October 28, 2026

David B. Hinchman
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Hinchman:

Attached are comments on the U.S. Government Accountability Office's (GAO) draft report entitled, **"CRITICAL INFRASTRUCTURE PROTECTION: Further Action Needed to Enhance Cybersecurity of the Food and Agriculture Sector"** (GAO-27-108656).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Gary Andres
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED – CRITICAL INFRASTRUCTURE PROTECTION: FURTHER ACTION NEEDED TO ENHANCE CYBERSECURITY OF THE FOOD AND AGRICULTURE SECTOR (GAO-27-108656)

The Department appreciates the opportunity to review and comment on this draft report.

GAO Recommendation 3
The Secretary of Health and Human Services should ensure that the Director of the Food and Drug Administration's Office of Coordinated Outbreak Response, Evaluation, & Emergency Preparedness fully implements the SRMA requirement related to information sharing of cybersecurity threats and vulnerabilities with CISA, including by assessing whether resources should be reprioritized or requested to continuously collect information on cybersecurity threats.

HHS Response
FDA concurs with the recommendation. The Director for the FDA Office of Coordinated Outbreak Response, Evaluation & Emergency Preparedness (CORE+EP) should share appropriate and pertinent information regarding cybersecurity threats and vulnerabilities with CISA and assess related resource prioritization and requests. The CORE+EP Director is also reviewing the flow of information from CISA and FBI and considering cybersecurity monitoring processes and related analyses.

GAO Recommendation 4
The Secretary of Health and Human Services should ensure that the Director of the Food and Drug Administration's Office of Coordinated Outbreak Response, Evaluation, & Emergency Preparedness fully implements the SRMA requirement related to facilitating or conducting cybersecurity emergency preparedness exercises and simulations, including by assessing whether resources should be reprioritized or requested to do so.

HHS Response
FDA concurs with the recommendation. The CORE+EP Office Director is considering a portfolio of potential work to include both cybersecurity planning documents and preparedness exercises. FDA also notes ongoing willingness to participate in interdepartmental cybersecurity exercises and simulations, as is evidenced by previous participation in the Department of Homeland Security exercise "Cyber Storm IX."

GAO Recommendation 5
The Secretary of Health and Human Services should ensure that the Director of the Food and Drug Administration's Office of Coordinated Outbreak Response, Evaluation, & Emergency Preparedness fully implements the SRMA requirement related to developing planning documents for coordinated action in the event of cybersecurity disasters or emergencies.

HHS Response
FDA concurs with the recommendation. The CORE+EP Office Director is initiating plans to meet this recommendation, including development of planning documents for coordinated action in the event of a cybersecurity incident. FDA notes that the Director is also considering adding such scenarios, when finalized, to the FDA webpage on food-related emergency exercise scenarios. This consideration, and associated activities, may fall under efforts outlined in FDA's response to GAO Recommendation 4.

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

David B. Hinchman, HinchmanD@gao.gov

Staff Acknowledgments

In addition to the individual named above, the following staff made key contributions to this report: Michael W. Gilmore (Assistant Director), Kavita Daitnarayan (Analyst in Charge), Smith Julmisse, Jess Lionne, Dwayne Staten, and Ibrahim Suleman.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday, GAO posts on its website newly released reports, testimonies, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Connect with GAO

Connect with GAO on X, LinkedIn, Instagram, and YouTube.
Subscribe to our Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us



Please Print on Recycled Paper.