

Foreign Ownership, Control, and Influence (FOCI) Risks in the Food and Agriculture Sector

June 13, 2024

Congressional Research Service

<https://crsreports.congress.gov>

R48094



R48094

June 13, 2024

Brian E. Humphreys
Analyst in Science and
Technology Policy

Foreign Ownership, Control, and Influence (FOCI) Risks in the Food and Agriculture Sector

In recent years, congressional concerns over potential risks to domestic food security posed by foreign ownership, control, and influence (FOCI) of critical infrastructure in the U.S. food and agriculture sector (FA Sector) have grown. FA Sector critical infrastructure encompasses many elements of the nation's food supply chain. Examples include farms, grain elevators, certain testing laboratories, meatpacking facilities, and supermarkets.

The U.S. Department of Agriculture (USDA) and the Food and Drug Administration (FDA) are the designated Sector Risk Management Agencies (SRMAs) for the FA Sector (1 of 16 federally designated critical infrastructure sectors). The SRMAs identify four main categories of risk to FA Sector-related functions: food contamination and disruption (accidental or intentional), disease and pests, severe weather, and cybersecurity. Partnerships are premised on the overarching assumption that private-sector owners of critical systems and assets are good-faith actors in a shared enterprise focused on ensuring availability and continuity of “national critical functions.”

However, FOCI risks more often relate to the control, exploitation, or malicious use of otherwise operable systems and assets by self-interested foreign adversaries—instances where the good faith of asset owners cannot be assumed. This type of risk has not been consistently or systematically assessed within the existing critical infrastructure security and resilience (CISR) voluntary partnership framework. Potential FOCI risks in the FA Sector include prioritization of foreign markets over domestic food security considerations; intellectual property (IP) theft of strategically important genetic engineering research; illicit or forced technology transfer; control of agricultural land and basic agricultural inputs; access to sensitive infrastructure information (e.g., vulnerability assessments based on voluntary disclosures by private-sector entities); and control of critical cyber systems, assets, and networks.

The Biden Administration has released several policy directives that address various infrastructure and supply chain issues specific to the FA Sector or—more broadly—to FOCI risks affecting multiple sectors. This includes a 2022 National Security Memorandum (NSM), “Strengthening the Security and Resilience of United States Food and Agriculture” (NSM-16), which contains provisions that expand federal regulatory reviews of foreign acquisitions of agricultural firms to include food security (in addition to national security) and that mandate supply chain security assessments by federal agencies (including USDA in the FA Sector).

Many recent assessments note trends toward consolidation and foreign ownership within key segments of U.S. agriculture. For example, a USDA report identified the growing ownership concentration in meat and poultry manufacturing, pesticides and crop seeds, and farm machine parts as sources of potential supply chain risk, although it did not specifically identify FOCI as a factor. A 2021 joint report on FA Sector risks by the Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI) warned of the possibility of a “takeover of [an] important supply chain entity by foreign investors” as part of an economic coercion and manipulation campaign. Foreign-owned or -controlled multinationals already have large, legally acquired holdings in various FA Sector segments.

Some Members of Congress have expressed concern about the People's Republic of China's (PRC's) acquisition of major food processing and agrochemical firms that have significant market share in the United States. Some public interest groups allege that multinationals may abuse IP protections for agrochemicals and genetically engineered seed, effectively control use of agricultural land, and gain access to farm-level data. Multinationals counter that IP protections allow for investments in new technologies and provision of innovative products at affordable prices to U.S. food producers. Foreign acquisitions of U.S. farmland have also caused concern, prompting legislative proposals that would restrict certain acquisitions. According to USDA, as of December 31, 2022, foreign entities—mainly Canada and some Western European countries—held an interest in 44.3 million acres of U.S. agricultural land, or about 3.4% of the total. PRC-linked holdings are small by comparison but have garnered scrutiny.

Policy options for Congress exist in several areas related to FOCI risks in the FA Sector. These areas include (1) federal reviews of foreign investments and acquisitions of FA Sector assets, (2) requirements for data and reporting of foreign land purchases, (3) resourcing of SRMA programs and activities, (4) assessments of FOCI risk, and (5) IP protections in the bioeconomy and farming.

Contents

Introduction	1
Background: The Food and Agriculture Sector	2
Risk Management in the FA Sector.....	3
SRMA Organization and Resourcing for FA Sector Engagements	4
DHS Leadership and Coordination	6
Related Programs, Policies, and Directives	7
National Security Memorandum for the FA Sector.....	7
Executive Order on Bioeconomy	9
Executive Order on CFIUS	10
Executive Order on America’s Supply Chains.....	10
Prospective Cyber Incident Reporting Requirements	11
Potential FOCI Risks in the FA Sector	11
Supply Chain Security.....	11
Foreign Acquisition of Seed and Agricultural Chemical Suppliers	12
Foreign Acquisition of Meat and Poultry Suppliers	13
Food Processing, Packaging, and Production	14
Agricultural and Food Supporting Facilities	14
Regulatory, Oversight, and Industry Organizations	15
The Role of Transnational Criminal Organizations	15
Foreign Control of U.S. Farmland	16
Land Ownership Risks.....	16
Technology Use Agreements for Basic Agricultural Inputs.....	17
Conclusion.....	18

Tables

Table 1. Agency Deliverables in “National Security Memorandum on Strengthening the Security and Resilience of United States Food and Agriculture” (NSM-16)	9
--	---

Contacts

Author Information.....	20
-------------------------	----

Introduction

In recent years, congressional concerns have grown over potential risks to domestic food security posed by foreign ownership, control, and influence (FOCI) of critical infrastructure in the U.S. food and agriculture sector (FA Sector). *Critical infrastructure* is defined in statute as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”¹ Critical infrastructure systems and assets in the FA Sector encompass many elements of the nation’s food supply chain. Examples include farms, grain elevators, farm supply wholesalers, certain testing laboratories, meatpacking facilities, bars and restaurants, and supermarkets.²

The national critical infrastructure security and resilience (CISR) enterprise combines both varying degrees of regulation and voluntary public-private partnerships for information sharing and best practices.³ The Department of Homeland Security (DHS) coordinates national strategy, interagency activities, and public-private partnerships for infrastructure security and resilience. DHS delegates sector leadership to other federal agencies in some cases, including the FA Sector. The FA Sector is 1 of 16 designated critical infrastructure sectors under current presidential directives.⁴

CISR programs and activities in the FA Sector are led by the U.S. Department of Agriculture (USDA) and Food and Drug Administration (FDA), which are the FA Sector’s designated Sector Risk Management Agencies (SRMAs). Public-private partnerships are largely voluntary and are premised on the overarching assumption that private-sector owners of critical systems and assets are good-faith actors in a risk management enterprise focused on protecting critical systems and assets and the functions they enable.⁵ USDA and FDA identify four main categories of risk to FA Sector-related functions: food contamination and disruption (accidental or intentional), disease and pests, severe weather (i.e., droughts, floods, and climate variability), and cybersecurity.⁶

FOCI risks in the FA Sector are not associated with the incapacity or destruction of critical systems and assets or disruption of essential functions. More often, FOCI risks relate to the

¹ The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act (P.L. 107-56). The FA Sector is 1 of 16 designated critical infrastructure sectors under current presidential directives. For information on the critical infrastructure risk management framework, see Department of Homeland Security (DHS), *The National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*, Washington, DC, 2013; and Food and Drug Administration (FDA), U.S. Department of Agriculture (USDA), and DHS, *Food and Agriculture Sector-Specific Plan*, 2015, pp. 5-7, <https://www.usda.gov/sites/default/files/documents/2015-food-and-agriculture-sector-specific-plan.pdf> (hereinafter FA SSP).

² See Appendix 6, FA SSP. According to the DHS Cybersecurity and Infrastructure Security Agency (CISA), the FA Sector has critical dependencies with several other designated critical infrastructure sectors, including Water and Wastewater Systems, Transportation Systems, Energy, and Chemical. However, an examination of foreign ownership risks in these sectors and their potential applicability to the FA Sector is beyond the scope of this report. Likewise, this report does not cover foreign ownership of systems, assets, and networks outside U.S. jurisdiction or imports of essential foreign-sourced agricultural production materials into the United States.

³ See White House, “National Security Memorandum on Critical Infrastructure Security and Resilience,” (NSM-22), presidential memorandum, April 30, 2024, <https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience>.

⁴ Ibid.

⁵ FA SSP.

⁶ For information on the critical infrastructure risk management framework, see DHS, *The National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*, Washington, DC, 2013, and FA SSP, pp. 5-7.

control, exploitation, or malicious use of productive systems and assets by self-interested foreign adversaries—instances where the good faith of asset owners cannot be assumed. This type of risk has not been consistently or systematically assessed within the existing CISR voluntary partnership framework.

Potential FOCI risks in the FA Sector identified in this report include prioritization of foreign markets over domestic food security considerations; intellectual property (IP) theft of strategically important genetic engineering research; illicit or forced technology transfer; control of agricultural land and basic agricultural inputs; access to sensitive infrastructure information (e.g., vulnerability assessments based on voluntary disclosures by private-sector entities); and control of critical cyber systems, assets, and networks.

This report provides analysis of potential FOCI risks in the FA Sector and the bearing these risks might have on the overall security and resilience of the sector. The report also provides options for congressional legislation and oversight.

Background: The Food and Agriculture Sector

Presidential directives established critical infrastructure sectors that encompass broad areas of the economy, government, and public services.⁷ There are currently 16 sectors and numerous subsectors. The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY2021 NDAA; P.L. 116-283) defined the role of SRMAs.⁸ In each sector, SRMAs chair the Government Coordinating Councils (GCCs), which provide for coordination among interagency and intergovernmental partners. Sector Coordinating Councils (SCCs) operate as counterparts to the GCCs, representing the interests of private-sector partners and other nongovernmental stakeholders within a given sector. SCCs are voluntary, self-organized, and self-governing bodies, often chaired by private-sector industry leaders.

The Department of Health and Human Services (HHS), acting through FDA, and USDA are the designated co-SRMAs for the FA Sector. FA SCC membership is composed of major industry enterprises and trade groups.⁹ Most sectors have a recognized Information Sharing and Analysis Center (ISAC), which serves as a hub for threat reporting, analysis, and information sharing with sector partners on cybersecurity and other matters.

The FA Sector's ISAC was originally formed in 2002 but closed in 2008 after failing to attract an active user base.¹⁰ Sector stakeholder interests were then represented by the Food and Ag Special Interest Group (SIG) within the Information Technology (IT) ISAC. Some observers criticized

⁷ White House, "National Security Memorandum on Critical Infrastructure Security and Resilience" (NSM-22), presidential memorandum, April 30, 2024, <https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/>.

⁸ See Section 9002, "Sector Risk Management Agencies." These coordinating bodies are chartered under Critical Infrastructure Protection and Advisory Council (CIPAC) auspices. CIPAC authorities, originally established by DHS in 2006 pursuant to the Homeland Security Act of 2002 (P.L. 107-296), afford certain exemptions from public reporting of meetings and disclosure of sensitive infrastructure information. See DHS, "Critical Infrastructure Partnership Advisory Council," 71 *Federal Register* 14930, March 24, 2006.

⁹ For a full list of FA Sector Coordinating Council membership and links to the current charter, see CISA, "Food and Agriculture Sector: Council Charters and Membership," <https://www.cisa.gov/food-and-agriculture-sector-council-charters-and-membership>.

¹⁰ The Food Marketing Institute, an industry group, established an agriculture Information Sharing and Analysis Center (ISAC) in 2002 prior to the establishment of DHS as an agency but disbanded it in 2008 due to "lack of activity and information flow," according to media reports. See "Food Sector Abandons Its ISAC," *Security Management*, September 1, 2008, <https://www.asisonline.org/security-management-magazine/articles/2008/09/food-sector-abandons-its-isac/>.

this arrangement as inadequate to the scale of cyber threats faced by the FA Sector.¹¹ Industry leaders rebranded the Food and Ag SIG as the Food and Agriculture Sector ISAC in 2023.¹² Although the new ISAC continued to operate under IT-ISAC auspices, its leaders asserted that the change would raise the profile of the organization and clarify its mission.¹³ Separately, in 2022, DHS sponsored preliminary development of a state-level pilot ISAC for FA Sector issues through the National Agriculture Biosecurity Center at Kansas State University.¹⁴

Policy options for Congress include whether current information-sharing organizations are appropriately organized and have the necessary resources to meet FA Sector cybersecurity and other security needs, as well as legislation to create new information-sharing organizations.¹⁵

Risk Management in the FA Sector

SRMAs consider a wide range of plausible man-made and natural hazard events that could negatively affect availability and continuity of critical infrastructure functions.¹⁶ CISR programs and activities in the FA Sector to date have been limited in scale and centered on traditional agency missions, such as maintaining the national food safety system and safeguarding farm production of raw foodstuffs from contamination.

FOCI risks affecting food and agriculture may be addressed through national security reviews of certain covered foreign investment transactions, including mergers and acquisitions, by the interagency Committee on Foreign Investment in the United States (CFIUS)—CFIUS authorities are governed by Section 721 of the Defense Production Act of 1950 (P.L. 81-774), as amended. CFIUS may recommend that the President block certain foreign investments, including those that would result in foreign control of any critical infrastructure, if it determines that the transaction would threaten to impair U.S. national security and the risk cannot be mitigated. CFIUS may review certain covered foreign investment and real estate transactions involving the acquisition of

¹¹ See Eric Geller, “The Dangerous Weak Link in the U.S. Food Chain,” *Wired*, April 6, 2023, <https://www.wired.com/story/us-food-agriculture-isac-cybersecurity/>. The Food and Agriculture Industry Cybersecurity Support Act, introduced in the 118th Congress (S. 2393 and H.R. 1219), would mandate creation of a cybersecurity clearinghouse for the sector hosted by the National Telecommunications and Information Administration, a Department of Commerce agency.

¹² Food and Ag ISAC (an IT ISAC Community), “Built by Industry for Industry,” <https://www.foodandag-isac.org/>; and “Food and Ag-ISAC Forms to Protect Agrifood Sector from Cybersecurity Threats,” *Food Safety Magazine*, May 26, 2023, <https://www.food-safety.com/articles/8617-food-and-ag-isac-forms-to-protect-agrifood-sector-from-cybersecurity-threats>.

¹³ Tim Starks, “The Food and Agriculture Industry Gets a New Center to Share Cybersecurity Information,” *Washington Post*, May 24, 2023, <https://www.washingtonpost.com/politics/2023/05/24/food-agriculture-industry-gets-new-center-share-cybersecurity-information/>.

¹⁴ FDA, USDA, DHS, *Food and Agriculture Sector Annual Report: Fiscal Year 2022*, p. 17, <https://www.fda.gov/media/171959/download>; Kansas State University, “Creation of a Kansas Food and Agriculture Information Sharing and Analysis Organization,” <https://www.k-state.edu/govrelations/federal/NABC-CreationofaKansasFoodandAgricultureInformationSharingandAnalysisCenter.pdf>.

¹⁵ Representative Pfluger introduced a bill in the 118th Congress, “Food and Agriculture Industry Cybersecurity Support Act” (H.R. 1219), which directs the Government Accountability Office to report on the feasibility of creating a dedicated FA Sector ISAC.

¹⁶ CISA defines a set of 55 National Critical Functions as “functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”

agricultural land and corporate entities, and may consider “elements of the agriculture industrial base that have implications for food security.”¹⁷

However, the range of transactions CFIUS covers is relatively narrow, focusing on national security risks of corporate acquisitions, noncontrolling investments, and real estate transactions, rather than CISR writ large. Options for Congress include legislation to expand CFIUS jurisdiction over transactions in the FA Sector and to add the Secretary of Agriculture as a full member of CFIUS.¹⁸ Another option is to provide USDA with additional appropriations to fund expansion of CFIUS-related programs and activities to cover a wider range of FOCI risks in the FA Sector.

SRMA Organization and Resourcing for FA Sector Engagements

USDA SRMA responsibilities reside with USDA’s National Security Division within the Office of Homeland Security (OHS). The division oversees the agency’s programs and participation in interagency activities, which may include FOCI-related risk management activities under programs such as CFIUS, Critical Infrastructure and Insider Threat, Foreign National Vetting, Intelligence, and FA Sector.¹⁹ FDA SRMA responsibilities reside with the Office of Analytics and Outreach/Food Defense and Emergency Coordination Staff at the Center for Food Safety and Applied Nutrition (CFSAN). Neither USDA/OHS nor FDA/CFSAN receives dedicated appropriations for SRMA-related programs and activities. Instead, SRMA engagement appears to be carried out in addition to other customary activities included in these offices’ program portfolios.²⁰

USDA requested \$225,000 in funds to support OHS engagements with FA Sector stakeholders in its FY2024 budget request.²¹ Referencing a ransomware attack on JBS—a Brazilian-owned meat processing firm with extensive operations in the United States—USDA/OHS stated that as “cybersecurity threats and vulnerabilities continue to grow, USDA is unable to conduct ... SRMA responsibilities[,] which could have a significant impact on the safety and security of U.S. agriculture” because of a lack of dedicated appropriations for this purpose.²² The FDA budget

¹⁷ Executive Order (E.O.) 14083, “Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States,” 87 *Federal Register* 57369, September 15, 2022. Committee on Foreign Investment in the United States (CFIUS) reviews may involve consultation with a designated USDA official. CFIUS is an interagency body comprising nine Cabinet members and others, as appointed. For more information on CFIUS authorities and activities, see CRS In Focus IF10177, *The Committee on Foreign Investment in the United States*, by Cathleen D. Cimino-Isaacs and Karen M. Sutter.

¹⁸ See CRS In Focus IF12312, *Foreign Ownership of U.S. Agriculture: Selected Policy Options*, by Renée Johnson.

¹⁹ See USDA, National Security Division, “National Security Division Related Topics,” <https://www.usda.gov/da/ohs/nsd>.

²⁰ Based on review of the FA SSP; USDA Office of Homeland Security (OHS), *2024 USDA Explanatory Notes*, 2023, <https://www.usda.gov/sites/default/files/documents/02-2024-OHS.pdf>; Department of Health and Human Services (HHS), *Food and Drug Administration: Justification of Estimates for Appropriations Committees*, 2023, <https://www.fda.gov/media/166182/download>; FDA, “Food Defense,” <https://www.fda.gov/food/food-defense>; and FDA, “What We Do at CFSAN,” <https://www.fda.gov/about-fda/center-food-safety-and-applied-nutrition-cfsan/what-we-do-cfsan>.

²¹ See USDA OHS, *2024 USDA Explanatory Notes*, p. 2-7; and Geller, “The Dangerous Weak Link in the U.S. Food Chain.” Geller notes, “By comparison, the Energy Department requested \$245 million for its Office of Cybersecurity, Energy Security, and Emergency Response.”

²² USDA OHS, *2024 USDA Explanatory Notes*, p. 2-7.

justification for FY2025 does not show any dedicated SRMA appropriations for FA Sector activities.²³

USDA and FDA list FA Sector engagement activities in annual Food and Agriculture Sector Specific Plan (FA SSP) progress reports, including exercises with FA Sector stakeholders.²⁴ The exercises include several food defense emergency scenarios but do not include FOCI-related threats or other FOCI issues that might affect emergency response. In April 2024, the Cybersecurity and Infrastructure Security Agency (CISA) hosted the Cyber Storm IX exercise, a major national cybersecurity exercise, which focused on the FA Sector as a possible target of cyberattacks.²⁵ The extent to which potential FOCI-related vulnerabilities or threats were incorporated into the exercise scenario is not clear.²⁶

The USDA Office of Inspector General (OIG) has participated in the interagency Foreign Influence Investigations Working Group, but it is not clear what the scope of the activity was or whether the group is still active.²⁷ Some former agency officials and infrastructure protection experts have publicly voiced general concerns about the scope and effectiveness of FA Sector SRMA engagements with key stakeholders, according to media reports, although these concerns do not appear to be specific to management of FOCI risks.²⁸

USDA is not an official member of CFIUS but is sometimes brought in at the Treasury Department's discretion on certain transactions. Some Members of Congress have argued that USDA should be a full member given the number of CFIUS cases and sensitive foreign acquisitions involving agriculture, biotechnology, and other USDA equities.²⁹ USDA/OHS currently has one staff member fully dedicated to CFIUS, according to the agency's FY2024 budget justification. USDA requested an additional \$500,000 and two full-time employees in anticipation of a potential increase in the scope of CFIUS activity, to include a wider array of agriculture-related transactions. According to its FY2024 budget justification, USDA concluded an agreement with the Treasury Department, giving it "enhanced access" to CFIUS cases that "requires additional OHS and [Office of the General Counsel] resources to ensure we support the

²³ HHS, Food and Drug Administration, *Justification of Estimates for Appropriations Committees: Fiscal Year 2025, 2024*, <https://www.fda.gov/media/176925/download>.

²⁴ See DHS, *Food and Agriculture Sector Annual Report: Fiscal Year 2021*, <https://www.fda.gov/media/165833/download>. FDA provides free emergency exercise scenarios for FA Sector stakeholders on its website, "Food Related Emergency Exercise Bundle (FREE-B) Download," <https://www.fda.gov/food/food-defense-tools/food-related-emergency-exercise-bundle-free-b-download>. The content is listed as current as of March 5, 2024.

²⁵ See Jen Easterly, "Prepared Together—Cyber Storm IX Recap," Cybersecurity and Infrastructure Security Agency (CISA), May 16, 2024, <https://www.cisa.gov/news-events/news/prepared-together-cyber-storm-ix-recap>. According to Jen Easterly, the CISA Director, "Participating organizations worked directly with CISA and coordinating bodies such as Sector Risk Management Agencies and Information Sharing and Analysis Centers to understand roles and capabilities during a cyberattack."

²⁶ CISA has released after-action reports for past Cyber Storm exercises, typically several months after their conclusion. No after-action report for Cyber Storm IX is available as of this writing.

²⁷ See FY2021 FA SSP annual progress report, and USDA Office of Inspector General, *Semiannual Report to Congress: Second Half April 1, 2022–September 30, 2022*, no. 88, October 2022, p. 32, https://usdaoig.oversight.gov/sites/default/files/reports/2023-12/SARC_FY%25202022_Second%2520Half_508.pdf.

²⁸ Geller, "The Dangerous Weak Link in the U.S. Food Chain." For example, Geller quotes Mark Montgomery, former executive director of the Cyberspace Solarium Commission, as saying that USDA as co-SRMA is "significantly less effective" than other SRMAs. Brian Harrell, a former assistant director for infrastructure security at CISA, is quoted as saying that the FA Sector needs its own ISAC to provide "a true operational assessment."

²⁹ For example, Congressman Frank Lucas, "Lucas Legislation Addressing Foreign Land Acquisition Passes Through Committee," press release, September 29, 2023, <https://lucas.house.gov/posts/lucas-legislation-addressing-foreign-land-acquisition-passes-through-committee>.

agreement between Departments. Previously USDA reviewed less than 50 CFIUS cases annually, and since August 2022, our workload has increased to over 250 cases.”³⁰

Options for Congress include requesting additional information about the scope and extent of FDA and USDA activities to support CISR (and specifically FOCI) risk management programs and activities in the FA Sector and providing appropriations to support additional SRMA engagement with the FA Sector. A potential oversight question for Congress could be whether FOCI-related risks are included in relevant exercise scenarios provided by SRMAs (see above). Congressional oversight could also include examination of reports and data on sector engagement from the relevant FA Sector SRMAs—to include appropriate quantifiable metrics and criteria of success. Greater overall engagement with industry stakeholders may clarify what, if any, differences exist between the rate and quality of foreign- and U.S.-owned firms’ participation in public-private partnerships and the nature of those differences.

DHS Leadership and Coordination

DHS is responsible for overall coordination of federal CISR activities. It maintains food and agriculture defense programs and activities through the Office of Health Security to support the FA Sector according to legislative requirements and executive branch policy directives.³¹ In addition, DHS previously provided grant funding to the University of Minnesota Center of Excellence for food protection and defense, which now operates independently as the Food Protection and Defense Institute. The institute supports interdisciplinary research on protection of the global food supply, “including supply chain resilience, information sharing, risk analysis and assessment, education, epidemiology, [and] economics,” among other topics.³²

In 2019, CISA introduced National Critical Functions as a conceptual framework for identifying and assessing cross-sector risk to essential or systematically important infrastructure systems, assets, and networks, to complement and expand the existing sector-based CISR framework. CISA defines National Critical Functions as

functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.³³

The 55 designated National Critical Functions include production and provision of agricultural products and services, and human and animal food products and services.³⁴

³⁰ USDA OHS, *2024 USDA Explanatory Notes*, pp. 2-7.

³¹ See DHS, *DHS Fact Sheet on National Security Memorandum-16 on Strengthening the Security and Resilience of United States Food and Agriculture*, 2022, https://www.dhs.gov/sites/default/files/2022-11/NSM_DHS%20FACT%20SHEET%20on%20NSM%20Food%20and%20Agriculture.pdf; also see DHS, Science and Technology Directorate (DHS S&T), “Food and Agriculture Defense,” <https://www.dhs.gov/science-and-technology/food-and-agriculture-defense>. According to the web page, “S&T’s food and agriculture defense work includes risk assessments; threat characterizations; countermeasures to defend against pathogens, pests, and toxins; food defense and ingestion threat modeling; characterizations of chemical threats for food contamination and adulteration; laboratory experiments and foundational research; diagnostics; veterinary medical countermeasures; decontamination strategies; trainings; and coordination with partners for joint efforts that defend food and agriculture systems.”

³² See University of Minnesota, Food Protection and Defense Institute, “Protecting the Global Food Supply Through Research, Education, and the Delivery of Innovative Solutions,” <https://foodprotection.umn.edu/>.

³³ See CISA, “National Critical Functions,” <https://www.cisa.gov/national-critical-functions>.

³⁴ See CISA, “National Critical Functions Set,” <https://www.cisa.gov/national-critical-functions-set>.

Related Programs, Policies, and Directives

The 2013 National Infrastructure Protection Plan (NIPP) and the FA SSP have provided the primary risk management guidance for FA Sector stakeholders over the past decade.³⁵ The FA SSP defines risk “in the context of the NIPP 2013 ... as the potential for loss, damage, or disruption to the Nation’s critical infrastructure resulting from destruction, incapacitation, or exploitation during some future manmade or naturally occurring event.”³⁶ These documents outline an organizational approach and framework for sector risk management—primarily through voluntary public-private partnerships—but generally do not direct specific agency actions. FA Sector Annual Reports provide updates on progress toward meeting FA SSP goals.³⁷ (The FA SSP and the subsequent annual progress reports do not specifically identify foreign ownership of agricultural land or sector assets as threats to the FA Sector.)

Section 9002 of the FY2021 NDAA (P.L. 116-283) directed the Secretary of Homeland Security to assess the current CISR policy framework and assess the need for changes to the existing critical infrastructure sectors. In November 2021, CISA submitted a statutorily mandated report on its assessment of the CISR framework and preliminary findings. It suggested, among other things, that the review process offered “an opportunity” to designate a Bioeconomy Sector separate from the existing FA Sector.³⁸ (The National Security Memorandum [NSM] on Critical Infrastructure Security and Resilience [NSM-22] retained existing sectors without modification but did not foreclose the possibility of new sectors in the future.) The bioeconomy is the portion of the economy based on products, services, and processes derived from biological resources (e.g., plants and microorganisms). Some of the FOCI risks in the FA Sector, such as IP protection of genetically engineered seed traits, relate to the bioeconomy.

Options for congressional action include oversight over DHS updates of its CISR policy framework as mandated in the FY2021 NDAA, to include changes to risk assessment scope and methods, and creation of a new Bioeconomy Sector. Another option would be oversight of executive branch programs and activities set forth in Executive Order (E.O.) 14017, NSM-16, NSM-22, Section 9002(b) of P.L. 116-283, and other laws, policies, and directives that may have a bearing on assessment of FOCI risks in the FA Sector.

National Security Memorandum for the FA Sector

On November 10, 2022, the White House released an NSM, “Strengthening the Security and Resilience of United States Food and Agriculture” (NSM-16), which covers the security and resilience of food and agriculture systems and supply chains; directs federal agencies to take actions to “identify and assess threats, vulnerabilities, and impacts” from high-consequence and catastrophic incidents; and prioritize resources “to prevent, protect against, mitigate, respond to,

³⁵ NSM-22 directs SRMAs to submit new sector-specific plans to the Secretary of Homeland Security within 270 days of issuance—January 25, 2025—and then biennially by February 1 of each year.

³⁶ FA SSP, p. 5.

³⁷ See FDA, “Food and Agriculture Sector and Other Related Activities: Food and Agriculture Sector Reports,” <https://www.fda.gov/food/food-defense-initiatives/food-and-agriculture-sector-and-other-related-activities>. The website has links to four FA Sector Annual Reports since 2015, for 2020, 2021, 2022, and 2023, respectively.

³⁸ CISA, *FY 2021 National Defense Authorization Act: Section 9002(b) Report*, November 12, 2021, p. 2, <https://www.cisa.gov/resources-tools/resources/section-9002b-report>. The term bioeconomy “refers to the share of the economy based on products, services, and processes derived from biological resources (e.g., plants and microorganisms). The bioeconomy is crosscutting, encompassing multiple sectors, in whole or in part (e.g., agriculture, textiles, chemicals, and energy).” See CRS Report R46881, *The Bioeconomy: A Primer*, by Marcy E. Gallo.

and recover from the threats and hazards that pose the greatest risk.”³⁹ It supersedes previous White House policy guidance given in Homeland Security Presidential Directive 9 (HSPD-9), issued in 2004.⁴⁰

NSM-16 identifies a wide range of threats facing sector stakeholders, to include chemical, biological, radiological, and nuclear (CBRN) threats; intentional introduction of hazardous contaminants; natural or genetically engineered pathogens and pests; and cybersecurity breaches leading to disruption of networked systems or IP theft. As with the earlier plans and directives, it does not specifically identify foreign ownership and control as a threat.

NSM-16 assigns primary responsibility for coordinating executive branch actions to the Assistant to the President for National Security Affairs (APNSA). The APNSA must provide an annual report to the President summarizing implementation progress, identifying capability gaps, and providing recommendations to close those gaps. Relevant provisions and reporting requirements are summarized in **Table 1**.

In March 2023, the FA Sector SRMAs and DHS jointly published the interim risk review mandated under NSM-16. The review contains a short section on foreign acquisitions in the FA Sector as a “potential factor contributing to risk,” which states:⁴¹

Foreign acquisition of U.S. agricultural assets may pose risks to the U.S. food and agriculture sector in some cases. For example, a recent research report prepared to support the deliberations of the U.S.-China Economic and Security Review Commission describes several potential risks to U.S. agriculture associated with recent acquisitions and attempted acquisitions of U.S.-based agricultural assets (including agricultural land, intellectual property [such as IP related to genetically modified seeds], and U.S.-based food producers and logistics companies), which may include loss of economic competitiveness, reduced exports, negative environmental impacts, and associated public health risks.⁴²

The review supports several other required assessment and planning products mandated by NSM-16 (see **Table 1**), which are in progress as of this writing, according to information posted on agency websites.⁴³

Three other relevant E.O.s preceded NSM-16—E.O. 14801 on the bioeconomy, E.O. 14083 related to CFIUS reviews, and E.O. 14017 on supply chain security and resilience. They are discussed below.

³⁹ See White House, “National Security Memorandum on Strengthening the Security and Resilience of United States Food and Agriculture,” presidential memorandum, November 10, 2022, <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/11/10/national-security-memorandum-on-on-strengthening-the-security-and-resilience-of-united-states-food-and-agriculture/>.

⁴⁰ White House, “Homeland Security Presidential Directive 9 (HSPD-9), Defense of United States Agriculture and Food,” presidential memorandum, January 30, 2004, <https://georgewbush-whitehouse.archives.gov/news/releases/2004/02/20040203-2.html>.

⁴¹ HHS, USDA, DHS, *National Security Memorandum on Strengthening the Security and Resilience of United States Food and Agriculture: 120-Day Food and Agriculture Interim Risk Review*, March 2023, p. 16, <https://www.fda.gov/media/170114/download>.

⁴² *Ibid.*, p. 22.

⁴³ See FDA, “National Security Memorandum on Strengthening the Security and Resilience of United States Food and Agriculture” (content current as of March 5, 2024), <https://www.fda.gov/food/food-defense/national-security-memorandum-strengthening-security-and-resilience-united-states-food-and>; and USDA, “Vulnerability Assessments” (content current as of July 31, 2023), <https://www.fsis.usda.gov/food-safety/food-defense-and-emergency-response/food-defense>.

Table 1. Agency Deliverables in “National Security Memorandum on Strengthening the Security and Resilience of United States Food and Agriculture” (NSM-16)

Department and Agency	Requirement	Timeline	Status
DOJ, DHS (in coordination with DOD and relevant agencies)	Provide threat assessment to leaders of relevant federal agencies on actors, threats, delivery systems, and methods that could be directed against the FA Sector.	Within 60 days (January 9, 2023) of publication of NSM-16, then annually.	No information
USDA, HHS, other relevant agencies (in coordination with FSLTT partners)	Conduct sector vulnerability assessment based on identified threats.	Within 180 days (May 9, 2023) of publication of NSM-16, then as needed.	In progress
DHS (in coordination with DOJ, USDA, HHS, and relevant agencies)	Provide comprehensive data-driven sector risk assessment informed by required threat and vulnerability assessments, prioritizing highest risks.	Within 1 year (November 10, 2023) of publication of NSM-16, then annually.	In progress
USDA, HHS (in coordination with relevant agencies)	Develop strategy and action plan based on risk assessment. Provide information on resilience capabilities, costs, and benefits; conduct risk mitigation analysis; and recommend research and development options to support mitigation.	Within 180 days of risk assessment completion, then revisions as needed.	In progress
USDA, HHS, DHS (in coordination with relevant agencies)	Conduct interim risk review on critical and emergent risks to FA Sector.	Within 120 days (March 10, 2023) of publication of NSM-16.	Published

Sources: CRS analysis of NSM-16 and U.S. Department of Agriculture (USDA) and Food and Drug Administration online updates.

Notes: DHS = Department of Homeland Security; DOD = Department of Defense; DOJ = Department of Justice; FA Sector = Food and Agriculture Sector; FSLTT = federal, state, local, territorial, and tribal; HHS = Department of Health and Human Services.

Executive Order on Bioeconomy

On September 12, 2022, President Biden issued E.O. 14081, “Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy.”⁴⁴ The E.O. focused on the economic potential of the bioeconomy and federal support of research and development (R&D), data sharing, workforce training, regulatory reforms, and other goals and objectives. In addition, it contained a security-related objective:

Secure and protect the United States bioeconomy by adopting a forward-looking, proactive approach to assessing and anticipating threats, risks, and potential vulnerabilities (including digital intrusion, manipulation, and exfiltration efforts by foreign adversaries), and by partnering with the private sector and other relevant stakeholders to jointly mitigate risks to protect technology leadership and economic competitiveness.

⁴⁴ E.O. 14801, “Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy,” 87 *Federal Register* 56849, September 15, 2022.

Accordingly, the E.O. instructed the APNSA and the Assistant to the President for Economic Policy to coordinate with the Secretaries of Defense and Agriculture and other agency leaders to identify actions to “mitigate risks posed by foreign adversary involvement in the biomanufacturing supply chain and to enhance biosafety, biosecurity, and cybersecurity in new and existing infrastructure.” Additionally, it required the Secretary of Homeland Security to conduct vulnerability assessments of bioeconomy-related critical infrastructure and National Critical Functions and to “enhance coordination with industry on threat information sharing, vulnerability disclosure, and risk mitigation for cybersecurity and infrastructure risks to the United States bioeconomy.”

For more information on E.O. 14081 and bioeconomy issues, see CRS Report R47274, *White House Initiative to Advance the Bioeconomy, E.O. 14081: In Brief*; CRS Report R46881, *The Bioeconomy: A Primer*; and CRS Report R47265, *Synthetic/Engineering Biology: Issues for Congress*.

Executive Order on CFIUS

On September 15, 2022, President Biden issued E.O. 14083, “Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States,” to update the factors taken into consideration in the CFIUS review process as part of ongoing implementation of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA; P.L. 115-232, Title XVII, Subtitle A).⁴⁵ E.O. 14083 notes that certain foreign investments “may undermine supply chain resilience efforts and therefore national security by making the United States vulnerable to future supply disruptions” and directs CFIUS to consider the effect of covered transactions on supply chain resilience and security, including with respect to “elements of the agriculture industrial base that have implications for food security,” among other sectors. For more information on E.O. 14083, see CRS In Focus IF12415, *CFIUS Executive Order on Evolving National Security Risks and CFIUS Enforcement Guidelines*.

Executive Order on America’s Supply Chains

On February 24, 2021, President Biden signed E.O. 14017, “America’s Supply Chains,” to ensure that supply chains are “resilient, diverse, and secure” against threats and hazards that might affect the “availability and integrity of critical goods, products, and services.”⁴⁶ It contains two requirements related to foreign investment issues (not specific to the FA Sector): (1) a progress report on developing domestic critical minerals supply chains and (2) recommendations for federal incentives and regulatory changes to encourage domestic and foreign investment in critical goods and materials. As with the more recent NSM, it assigns the White House coordination role to the APNSA. It requires each critical infrastructure sector SRMA to produce a report on relevant supply chain risks within one year. USDA, as co-SRMA in the FA Sector, published the required report (hereinafter the USDA supply chain report) in February 2022.⁴⁷

⁴⁵ E.O. 14083, “Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States,” 87 *Federal Register* 57369, September 15, 2022.

⁴⁶ E.O. 14017, “America’s Supply Chains,” 86 *Federal Register* 11849, March 1, 2021.

⁴⁷ USDA, *Agri-Food Supply Chain Assessment: Program and Policy Options for Strengthening Resilience*, Washington, DC, February 2022, <https://www.ams.usda.gov/supply-chain>.

Prospective Cyber Incident Reporting Requirements

In April 2024, DHS issued a proposed rule, “Cyber Incident Reporting for Critical Infrastructure Act Reporting Requirements.”⁴⁸ The proposed rule was issued in compliance with provisions of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), enacted under Division Y of the Consolidated Appropriations Act, 2022 (P.L. 117-103). It requires CISA to (1) engage in rulemaking to mandate reporting of cybersecurity incidents to the agency, (2) enforce noncompliance with required reporting, and (3) disseminate analysis based on the information collected. The FA Sector annual progress report for FY2022 noted that the FA Sector GCC and SCC “assisted in shaping the implementation” of CIRCIA requirements, without providing further detail.⁴⁹

According to P.L. 117-103, the reporting requirements apply to entities in federally designated critical infrastructure sectors “that [satisfy] the definition established by the Director in the final rule.” In designating covered entities, CISA proposed both general (e.g., size) and sector-based criteria. CISA declined to apply sector-based criteria to the FA Sector following consultations with the co-SRMAs.⁵⁰ Instead, CISA would apply a general size-based criterion to agricultural enterprises, which exempts small businesses from regulatory compliance, likely “based on the mean, median, or mode of number of employees across such entities.”⁵¹ According to CISA, the intent is to cover larger entities in the FA Sector to allow for development of “sector-specific threat and trends analysis.”⁵² The threat of state and non-state foreign adversaries was discussed throughout the proposed rule. However, the discussion did not include potential FOCI risks.

Potential FOCI Risks in the FA Sector

Supply Chain Security

A 2021 joint report on FA Sector risks by DHS, the Office of the Director of National Intelligence (ODNI), academics, and industry stakeholders (hereinafter the joint report) identified certain FOCI threats in agricultural supply chains.⁵³ Specifically, it identified the possibility of a “takeover of [an] important supply chain entity by foreign investors” as part of an economic coercion and manipulation campaign but did not elaborate on specific cases, threats, or acquisition mechanisms.⁵⁴ A 2022 report (hereinafter the Review Commission report) by the congressionally mandated U.S.-China Economic and Security Review Commission provided information on these and other issues as they related to China. The report stated that acquisition of major domestic agribusinesses may “confer undue leverage over U.S. supply chains” and lead to restructuring of supply chains that negatively affects domestic producers and service providers.⁵⁵

⁴⁸ DHS, “Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements,” 89 *Federal Register* 23644, April 4, 2024 (hereinafter CIRCIA rulemaking).

⁴⁹ FA SSP FY2022 update, p. 12, <https://www.fda.gov/media/171959/download>.

⁵⁰ CIRCIA rulemaking, p. 23702.

⁵¹ *Ibid.*

⁵² *Ibid.*, p. 23683.

⁵³ Office of the Director of National Intelligence and DHS, *Threats to Food and Agricultural Resources*, Washington, DC, 2021.

⁵⁴ *Ibid.*, p. 61.

⁵⁵ Lauren Greenwood, *Staff Research Report: China’s Interests in U.S. Agriculture: Augmenting Food Security* (continued...)

The Review Commission report also identified risks of IP theft, illicit technology transfer, and foreign control of domestic FA Sector supply chains. According to the report, these activities are part of a coordinated and deliberate policy of the government of the People's Republic of China (PRC) to address China's domestic food security challenges by increasing productivity through illicit technology transfer and overseas diversification of its agricultural supply chains.⁵⁶ In addition, the report warned that the PRC-linked firms may attempt to reverse-engineer illegally acquired U.S. seed varieties to identify vulnerabilities to crop disease and other threats.

The USDA supply chain report identified the growing ownership concentration in meat and poultry manufacturing, pesticides and crop seeds, and farm machine parts as sources of potential risk.⁵⁷ It did not specifically identify FOCI as a threat or risk factor. However, foreign-owned or -controlled multinationals have significant presence in these areas of production.

Foreign Acquisition of Seed and Agricultural Chemical Suppliers

In 2016, ChemChina announced plans to acquire Syngenta, a Swiss-based agricultural conglomerate (with extensive business operations in the United States) for \$43 billion.⁵⁸ The acquisition—claimed as the largest foreign acquisition by a PRC company at the time—became the subject of CFIUS review and was eventually approved.⁵⁹ While CFIUS reviews are not public, media reports suggested that the review would likely focus on defense-specific issues, such as proximity of Syngenta facilities to U.S. military bases and ownership of potentially sensitive military contracts, more than food-security-related FOCI issues.⁶⁰

In a press release following CFIUS's approval of the transaction, Senator Grassley (IA) stated

It's clear that China is looking at purchasing companies with food production expertise as part of a long-term strategic plan and a component of their national security. We need to be looking at these mergers in the same way, so it makes sense for CFIUS to take that angle

Through Investment Abroad, U.S.-China Economic and Security Review Commission, May 26, 2022, p. 3, <https://www.uscc.gov/annual-report/2022-annual-report-congress>.

⁵⁶ The government of the People's Republic of China has released national-level strategies in recent years highlighting acquisition of biotechnology from foreign firms as a priority. For more information, see CRS In Focus IF11684, *China's 14th Five-Year Plan: A First Look*, by Karen M. Sutter and Michael D. Sutherland.

⁵⁷ According to the report, "In 2019, the four largest fed cattle processing companies accounted for 85 percent of the total U.S. annual slaughter; the four largest hog processing companies accounted for 67 percent of the total annual hog slaughter; and the four largest chicken processing companies accounted for 53 percent of the total annual slaughter." See USDA, *Agri-Food Supply Chain Assessment: Program and Policy Options for Strengthening Resilience*, Washington, DC, February 2022, p. 13.

⁵⁸ Syngenta is one of the four largest suppliers of crop seeds and agricultural chemicals in the United States, according to the USDA Economic Research Service. See USDA Economic Research Service, "Two Companies Accounted for More than Half of Corn, Soybean, and Cotton Seed Sales in 2018-2020," <https://www.ers.usda.gov/data-products/chart-gallery/gallery/chart-detail/?chartId=107516>.

⁵⁹ Michael Shields, "ChemChina Clinches Landmark \$43 Billion Takeover of Syngenta," Reuters, May 5, 2017, <https://www.reuters.com/article/idUSKBN1810CM/>; Shangjing Li, "Simpson Thacher Helps ChemChina Obtain CFIUS Clearance for \$43 Bln Syngenta Buy," *Asian Legal Business*, August 26, 2016, <https://china.legalbusinessonline.com/node/73060>; ChemChina and Syngenta, "ChemChina and Syngenta Receive Clearance from the Committee on Foreign Investment in the United States," press release, August 22, 2016, <https://www.syngenta.com/sites/syngenta/files/press-release-pdf/2017/20160822-en-joint-release.pdf>.

⁶⁰ Diane Bartz, "ChemChina, Syngenta to Move Quickly on U.S. National Security Review," Reuters, February 3, 2016, <https://www.reuters.com/article/idUSKCN0VD03C/>; "'No Security Issues' in Syngenta Sale to China," *CHEManager International*, July 4, 2016, <https://www.chemanager-online.com/en/news/no-security-issues-syngenta-sale-china>.

into consideration when reviewing these transactions. The fact that a state-owned enterprise may have yet another stake in U.S. agriculture is alarming.⁶¹

In 2020, ChemChina and Sinochem—a Chinese state-owned multinational chemical manufacturing conglomerate—consolidated their agricultural assets into Syngenta.⁶² In response, some Members of Congress called upon the Treasury Secretary, as chair of CFIUS, to include food security issues in assessments of any foreign acquisitions of FA Sector entities.⁶³ In the 118th Congress, several bills under consideration would expand CFIUS reviews of foreign investment transactions in the FA Sector to include food security issues and would mandate regular USDA membership as opposed to informal, ad hoc participation.

The Consolidated Appropriations Act, 2024 (P.L. 118-42, §787), enacted in March 2024, requires the Secretary of Agriculture to be included as a member of CFIUS on a case-by-case basis with respect to covered transactions involving agricultural land, agriculture biotechnology, or the agriculture industry (including agricultural transportation, agricultural storage, and agricultural processing), as determined by the chair of CFIUS in coordination with the Secretary of Agriculture.⁶⁴ Congress provided \$2 million in appropriated funds, to remain available until expended, for USDA to implement this provision.

Foreign Acquisition of Meat and Poultry Suppliers

The MITRE Corporation noted in a July 2021 report (hereinafter the MITRE report) on domestic meat and poultry supply chains that some foreign-owned U.S. meat and poultry providers prioritized exporting meat products to their home country rather than supplying domestic consumption needs when spot shortages occurred during the COVID-19 public health emergency.⁶⁵ Further, the report recommended that FA Sector SRMAs and certain interagency partners identify foreign ownership of key processing and production facilities and analyze “the policy implications of non-compliance with U.S. government mandates during an emergency.”⁶⁶

Four major multinational agricultural companies control the majority of U.S. beef production. Two of these—JBS and National Beef Packing Company—are owned or controlled by Brazilian

⁶¹ Office of Sen. Chuck Grassley, “Grassley Statement on Conclusion of CFIUS Review of ChemChina-Syngenta Merger,” press release, August 22, 2016, <https://www.grassley.senate.gov/news/news-releases/grassley-statement-conclusion-cfius-review-chemchina-syngenta-merger>.

⁶² Reuters, “ChemChina, Sinochem Merge Agricultural Assets - Syngenta,” January 5, 2020, <https://www.reuters.com/article/idUSKBN1Z40HA/>.

⁶³ House Foreign Affairs Committee, “McCaul, Crawford Urge Treasury Department to Review Merger Between Chinese Government-Backed Military Companies,” press release, April 15, 2021, <https://foreignaffairs.house.gov/press-release/mccaul-crawford-urge-treasury-department-to-review-merger-between-chinese-government-backed-military-companies/>.

⁶⁴ Other legislation in the 118th Congress would broaden CFIUS’s authorities to review and potentially prohibit certain foreign purchases of real estate and/or agricultural land (e.g., H.R. 917/S. 369, H.R. 558, S. 1066, H.R. 1448, H.R. 4577, H.R. 5078/S. 2060), add USDA as a permanent CFIUS member agency (e.g., H.R. 683/S. 168, S. 2312, H.R. 3378, H.R. 4577, S. 2312, H.R. 5078/S. 2060), and expand the defined scope of U.S. critical infrastructure to explicitly include agricultural systems and supply chains (e.g., H.R. 513/S. 68).

⁶⁵ Bradford Brown et al., *U.S. Food Supply Chain Security: A Network Analysis*, MITRE Corporation, July, 2021, p. 4, <https://www.mitre.org/sites/default/files/2021-10/pr-21-1826-us-food-supply-chain-security-a-network-analysis.pdf>.

⁶⁶ *Ibid.*, p. 6.

entities.⁶⁷ Similarly, the acquisition of Smithfield Foods by WH Group Limited—a PRC firm—conferred control of 20% of the domestic pork processing industry to a foreign owner.⁶⁸

Reports that some foreign-owned meat processing plants prioritized deliveries to their home countries during the COVID-19 pandemic could also be a subject for congressional oversight and legislation.

Food Processing, Packaging, and Production

The MITRE report found that trends toward consolidation of entities were highly pronounced in the processing, packaging, and production of meat and poultry, creating a “dense and complex network” with several “key hubs” that were potentially vulnerable to disruption by man-made or natural causes.⁶⁹

With their high connectivity, these five key hubs have significant and extensive influence on the resilience and continuity of the U.S. meat supply chain. A disruption in any one of these hubs can have a large downstream effect on the rest of the network. The potential for disruption is further exacerbated by the network structure of “super embedded hubs” where each of these five key hubs are tightly interconnected.⁷⁰

The MITRE report considered several types of intentional threats to such hubs, to include biological, physical, or cyber-based attacks. The report did not specifically consider FOCI risks as they might relate to any of these types of attacks. It is not clear whether foreign-owned entities are more vulnerable to these attacks than their U.S.-owned counterparts or whether the fact of foreign ownership itself may be a threat in some cases. A report by the Food Protection and Defense Institute (hereinafter the FPD report) asserts that cybersecurity vulnerabilities, exacerbated by poor technical competence and a lax security culture, are widespread throughout FA Sector supply chains, but the FPD report does not attribute specific risks to FOCI threats in the FA Sector.

Although not specific to the FA Sector, E.O. 14083 of September 2022 states

investments by foreign persons with the capability and intent to conduct cyber intrusions or other malicious cyber-enabled activity—such as ... the operation of United States critical infrastructure ... may pose a risk to national security.

It is not yet clear whether FOCI risks to critical infrastructure identified in E.O. 14083 would fall within the scope of various risk management activities mandated in NSM-16, because the latter directive is still in the early implementation phase as of the date of this report (see “National Security Memorandum for the FA Sector” section).

Agricultural and Food Supporting Facilities

Agricultural and food supporting facilities include R&D facilities. The joint report states that these may be targeted by foreign entities for purposes of espionage, theft of trade secrets, and IP

⁶⁷ Christopher Walljasper, “More Foreign Ownership of U.S. Beef Processors Raises Food Safety Concerns,” *Investigate Midwest*, December 19, 2019, <https://investigatemidwest.org/2019/12/18/more-foreign-ownership-of-u-s-beef-processors-raises-food-safety-concerns/>.

⁶⁸ See Fitch Ratings, “Fitch Affirms Smithfield Foods, Inc.’s IDR at ‘BBB’; Outlook Stable,” October 10, 2022, <https://www.fitchratings.com/research/corporate-finance/fitch-affirms-smithfield-foods-inc-idr-at-bbb-outlook-stable-10-10-2022>.

⁶⁹ Bradford Brown et al., *U.S. Food Supply Chain Security: A Network Analysis*, p. 4.

⁷⁰ Ibid.

theft.⁷¹ Further, these activities may confer competitive advantages on foreign entities and provide “coercion points on aggressive corporate takeovers of U.S. corporations.”⁷² The joint report identifies “small and emerging corporations, universities, and government research organizations” as the most vulnerable entities of such targeting.⁷³

Regulatory, Oversight, and Industry Organizations

The USDA OIG noted investigations involving foreign influence or interference in the FA Sector in some recent reports to Congress. In its FY2022 (second half) semiannual report to Congress, the USDA OIG reported substantiated allegations of insider threat activity involving a senior official at USDA’s Animal and Plant Health Inspection Service (APHIS). Investigators found that the official maintained “inappropriate relationships” with foreign nationals, failed to report personal and official foreign travel, violated IT security, and accepted a gift from a foreign official without properly reporting it.⁷⁴ The FY2020 (first half) report noted that OIG audited USDA controls to prevent “unauthorized access to, and transfer of, USDA-funded research technology to foreign countries” by foreign research collaborators and found weaknesses that required correction by USDA agencies.⁷⁵ Semiannual USDA OIG reports for FY2023—the most recent available as of this writing—do not note any FOCI-related activities.

An option for Congress would be to exercise its oversight authorities to ascertain whether the recommended corrections suggested by USDA OIG to prevent further occurrences of IP theft by foreign entities were implemented. Another option for Congress would be to request the relevant OIG report in nonredacted form from USDA.

The Role of Transnational Criminal Organizations

A 2019 study included in the FPD I report found that FOCI threats in the FA Sector were not necessarily limited to otherwise legitimate business transactions. According to the FPD I study, “transnational criminal organizations (TCOs) are already heavily involved in large-scale food-related crimes such as counterfeiting, economically motivated adulteration, theft and resale, and smuggling.”⁷⁶ Further, cargo thefts are often aided by malicious cyber intrusions to penetrate agricultural supply chains and to identify and reconnoiter targets.⁷⁷

⁷¹ Office of the Director of National Intelligence and DHS, *Threats to Food and Agricultural Resources*, p. 26.

⁷² Ibid.

⁷³ Ibid.

⁷⁴ See USDA Office of Inspector General, *Semiannual Report to Congress: Second Half April 1, 2022–September 30, 2022*, no. 88, October, 2022, p. 87, https://usdaoig.oversight.gov/sites/default/files/reports/2023-04/SARC_FY%25202022_Second%2520Half_508.pdf. No motive was reported. Among other activities, the Animal and Plant Health Inspection Service (APHIS) has oversight responsibilities in animal health, biotechnology, imports and exports of food and plant products, and international services. The Department of Justice (DOJ) declined to prosecute the official; their security clearance was revoked by the agency.

⁷⁵ USDA Office of Inspector General, *Semiannual Report to Congress: First Half, October 1, 2019–March 31, 2020*, no. 83, May 2020, p. 5, https://usdaoig.oversight.gov/sites/default/files/reports/2023-04/sarc2020_1st_half_508.pdf. The public report was fully redacted. According to USDA, “Due to the nature of our findings and the agency’s responses, the report contains sensitive content. Thus, we are withholding it from public release due to concerns about the risk of circumvention of law.” See USDA Office of Inspector General, *USDA’s Controls to Prevent the Unauthorized Access and Transfer of Research Technology*, p. 1, <https://www.oversight.gov/sites/default/files/oig-reports/50701-0002-21.pdf>.

⁷⁶ Food Protection and Defense Institute, *The Cyber Risk to Food Processing and Manufacturing*, September 2019, p. 9, <https://conservancy.umn.edu/bitstream/handle/11299/217703/FPDI-Food-ICS-Cybersecurity-White-Paper.pdf>.

⁷⁷ Ibid.

In some cases, foreign-controlled firms have been targeted by TCOs for criminal exploitation or have themselves engaged in criminal practices. According to media reports, meat production by JBS facilities in the United States was disrupted in 2021 by a ransomware attack, which JBS attributed to a Russian TCO.⁷⁸ It is not clear whether foreign-owned entities are more vulnerable to these attacks than their U.S.-owned counterparts. The previous year, J&F Investimentos S.A., the Brazilian investment group that controls JBS,⁷⁹ pleaded guilty to violations of the Foreign Corrupt Practices Act as part of a bribery scheme in Brazil to obtain financing and other benefits and agreed to pay a \$256 million criminal penalty.⁸⁰

Foreign Control of U.S. Farmland

FOCI risks to U.S. farmland may involve direct ownership of the land or de facto control over land use for agricultural purposes, such as use of specific seed varieties and pesticides.

Land Ownership Risks

Increasing scarcity of arable land globally coupled with increasing demand for agricultural commodities has made U.S. farmland an attractive investment for certain foreign entities. Motivations for land acquisitions may be economic, strategic, or both. USDA tracks foreign acquisition of agricultural and nonagricultural land under authorities of the Agricultural Foreign Investment Disclosure Act of 1978 (AFIDA; P.L. 95-460). According to USDA, as of December 31, 2022, foreign persons and entities held an interest in 44.3 million acres of U.S. agricultural and nonagricultural land, accounting for 3.4% of total privately owned land.⁸¹

Owners from five countries (Canada, the Netherlands, Italy, the United Kingdom, and Germany) accounted for approximately 62% of all foreign-owned U.S. agricultural land in 2022. Other countries with aggregate owner holdings of more than 500,000 acres were Portugal, France, Denmark, Luxembourg, Mexico, Switzerland, the Cayman Islands, Japan, and Belgium. As of year-end 2022, USDA reports that PRC entities accounted for 383,935 acres, or 0.8%, of total foreign-owned U.S. agricultural land.⁸²

Ownership of U.S. agricultural land by PRC entities, as reported by USDA under AFIDA, appears negligible, accounting for less than 1% of total foreign-owned U.S. agricultural land as of year-end 2022. However, the Review Commission report raised concerns about the noncommercial purposes of PRC acquisitions (i.e., increasing China's food security) and the apparent acceleration of the pace of acquisitions, which have elicited concern both from Congress and

⁷⁸ Tom Polanske and Jeff Mason, "U.S. Says Ransomware Attack on Meatpacker JBS Likely from Russia," Reuters, June 1, 2021, <https://www.reuters.com/world/us/some-us-meat-plants-stop-operating-after-jbs-cyber-attack-2021-06-01/>.

⁷⁹ See JBS, "Ownership and Corporate," <https://ri.jbs.com.br/en/esg-investors/corporate-governance/ownership-and-corporate/>.

⁸⁰ DOJ, "J&F Investimentos S.A. Pleads Guilty and Agrees to Pay over \$256 Million to Resolve Criminal Foreign Bribery Case," press release, October 14, 2020, <https://www.justice.gov/opa/pr/jf-investimentos-sa-pleads-guilty-and-agrees-pay-over-256-million-resolve-criminal-foreign>.

⁸¹ CRS from USDA, *Foreign Holdings of U.S. Agricultural Land Through December 31, 2022* (Report 6), https://www.fsa.usda.gov/Assets/USDA-FSA-Public/usdfiles/EPAS/PDF/2022_afida_annual_report_12_20_23.pdf. Data cover sole foreign and joint U.S. ownership of privately held agricultural and nonagricultural land (out of a total of 1,290.5 million acres).

⁸² Ibid. For more background on the Agricultural Foreign Investment Disclosure Act of 1978 and foreign ownership of farm land, see CRS In Focus IF11977, *Foreign Ownership and Holdings of U.S. Agricultural Land*, by Renée Johnson, and CRS Report R47893, *Selected Recent Actions Involving Foreign Ownership and Investment in U.S. Food and Agriculture: In Brief*, by Renée Johnson.

from certain agricultural stakeholders and industry observers.⁸³ Legislation to restrict certain sales of agricultural land, tighten disclosure requirements, and expand federal review of foreign investment transactions has been introduced in recent Congresses.⁸⁴

Neither USDA, FDA, nor businesses associated with the FA Sector track or compile data on any associated farm assets and property conveyances that may be attached to the farmland ownership or property investment, such as buildings, equipment, machinery, livestock, and IP and other production-related or technology rights. This may create data gaps that complicate analysis of relevant events or trends. Congress may consider what data categories used for AFIDA disclosures are sufficient to identify FOCI-related risks to the FA Sector.

Technology Use Agreements for Basic Agricultural Inputs

Large agrochemical and seed firms—many foreign owned—commonly require customers to sign technology use agreements for use of seed and pesticides. Technology use agreements for patented seed varieties typically impose legally enforceable conditions on end users (farmers) that cover a range of common agricultural practices.⁸⁵ Some public interest groups and critics claim that the current patent system gives too much power to large firms, exceeds congressional intent, and allows for agency overreach in granting and enforcing IP rights.⁸⁶

“Ownership of [seed] biotech traits enable a level of control over every acre containing the trait,” one law firm wrote in response to a 2022 USDA request for public comment on competitiveness in the agricultural seed production business. “The contractual terms reach far beyond grants of [IP] rights and impose wide-ranging, intrusive, and often poorly defined, obligations and requirements on licensees.”⁸⁷

Enforcement clauses of technology use agreements may allow firms to have unrestricted access to licensees’ properties and facilities, business records (including receipts for chemicals and herbicides), internet service provider details, required crop-record submissions to USDA, and detailed records of farming practices (e.g., fertilizing, planting, and harvesting).⁸⁸ Violations may result in lawsuits or cancellation of use agreements, which may have the practical effect of cutting off access to seed supply for planting.

Some public interest groups assert that corporate collection and ownership of detailed data on farming practices may also raise fair data use and privacy issues. According to the American Antitrust Institute, “digital farming will likely enhance incentives to amass and appropriate valuable farm data for potential use as a strategic competitive asset.”⁸⁹

⁸³ See Review Commission report.

⁸⁴ For more information on recent legislation and policy development, see CRS In Focus IF12312, *Foreign Ownership of U.S. Agriculture: Selected Policy Options*, by Renée Johnson, and CRS Report R47893, *Selected Recent Actions Involving Foreign Ownership and Investment in U.S. Food and Agriculture: In Brief*, by Renée Johnson.

⁸⁵ For an overview of relevant legislation, court cases, and enforcement policies as presented to farmers, see Wisconsin Department of Agriculture, Trade and Consumer Protection, *What Is the U.S. Plant Variety Protection Act?* <https://datcp.wi.gov/Documents/BrownBagSeed.pdf>.

⁸⁶ For a public interest group perspective on congressional intent and other legal issues, see Debbie Barker et al., *Seed Giants vs. U.S. Farmers*, Center for Food Safety & Save Our Seeds, 2013, pp. 13-15, https://www.centerforfoodsafety.org/files/seed-giants_final_04424.pdf.

⁸⁷ Joel E. Cape, *Comments of Cape Law Firm*, Cape Law Firm, USDA Docket No. AMS-AMS-22-0025, June 15, 2022, pp. 2 and 4, <https://www.regulations.gov/comment/AMS-AMS-22-0025-0062>.

⁸⁸ Debbie Barker et al., *Seed Giants vs. U.S. Farmers*, p. 23.

⁸⁹ Diana L. Moss, *Comments of the American Antitrust Institute*, American Antitrust Institute, USDA Docket No. (continued...)

Because foreign-owned agrochemical and seed firms predominate in the U.S. market (see “Foreign Acquisition of Seed and Agricultural Chemical Suppliers” section), it follows that foreign-owned and -controlled entities may be able to amass detailed farm-level data—whether collected through IP enforcement activities or other means—across broad swaths of U.S. agricultural land.

Global agriculture firms assert that the patent system incentivizes and protects long-term R&D investments, which are necessary to produce seed traits such as those that have made higher crop yields possible over time at reasonable cost to farmers.⁹⁰ Additionally, they assert that acquisition of farm-level data facilitates development of precision agriculture products, as well as individualized recommendations for seed and herbicide use that benefit farmers.

In 2021, the Biden Administration directed USDA to prepare a report on consolidation within the agricultural seed industry, for which the agency subsequently sought public comment.⁹¹ Commenters—ranging from small organic farmers to major multinational conglomerates—noted the trend toward consolidation and globalization in the seed industry, the seed industry’s convergence with the agrochemical industry, and the increasing prevalence of seeds engineered to withstand various treatments (often sold by the same firms) against pests, weeds, and disease. In general, arguments centered on ecological, economic, and competitiveness concerns, rather than potential FOCI risks. Nonetheless, in some cases, foreign firms’ acquisitions of major seed producers have raised security concerns (see “Foreign Acquisition of Seed and Agricultural Chemical Suppliers” section).

Options for Congress include amending patent law to clarify its intent regarding the use of utility patents for genetically engineered seed traits and examining IP enforcement practices that foreign-owned firms may use to collect farm-level data and whether data are aggregated and used in ways that safeguard U.S. security interests.

Conclusion

FOCI within the U.S. FA Sector is widespread. Foreign-owned multinationals are present throughout the sector, in segments such as meat processing, agricultural chemicals, and crop seeds. Some foreign acquisitions of corporate entities or agricultural land may be subject to CFIUS review but are generally legal and generally allowed. In the R&D field, collaboration with foreign nationals and research institutions is commonplace in both the public and private sector. Further, the national CISR enterprise itself frequently relies on collaboration of U.S. public- and private-sector entities with their foreign counterparts. SRMAs generally assume that asset owners are good-faith actors, regardless of nationality.

However, FOCI may also present potential risks to the FA Sector, as seen in allegations of unauthorized technology transfer, theft or misappropriation of IP, prioritization of overseas markets over domestic demand, and attempted land purchases near sensitive military assets. Other potential areas of concern, such as farm-level data gathering by multinational firms and alleged

AMS-AMS-22-0025, May 16, 2022, p. 17, <https://www.antitrustinstitute.org/wp-content/uploads/2022/05/USDA-Comment-Agbiotech-6-10-22-REVISED-FINAL-FOR-AAI-WEBSITE.pdf>. Another nonprofit, The Open Markets Institute makes substantially similar arguments in its comments. See Open Markets Institute, *The Open Markets Institute’s Comments on “Competition and the Intellectual Property System: Seeds and Other Agricultural Inputs,”* May 16, 2022, pp. 5-7, <https://www.regulations.gov/comment/AMS-AMS-22-0025-0033>.

⁹⁰ For example, see Syngenta, “Intellectual Property & Regulatory,” <https://www.syngenta.com/en/about/faq/intellectual-property-regulatory>.

⁹¹ USDA Agriculture Marketing Service, “Competition and the Intellectual Property System: Seeds and Other Agricultural Inputs,” <https://www.regulations.gov/document/AMS-AMS-22-0025-0001>.

abuse of IP protections to control farming practices, relate primarily to concerns about corporate consolidation and concentration that are not specific to foreign ownership. Nonetheless, some Members of Congress and other observers have raised concerns over foreign acquisitions of U.S. and multinational firms in key FA Sector segments.

The full extent to which specifically *foreign* ownership, control, or influence over critical infrastructure systems and assets affects the overall level of risk to critical functions of the FA Sector (i.e., the safe production, distribution, and supply of food) has yet to be established. Much of the publicly available reporting is conjectural and anecdotal, complicating any more systemic analysis of FOCI risk to the FA Sector. Legislative mandates for data gathering on certain commercial transactions (e.g., AFIDA) and cybersecurity incident reporting (e.g., CIRCIA), as well as executive branch directives to appropriate federal agencies to conduct relevant studies, may offer an opportunity for more authoritative analyses.

Author Information

Brian E. Humphreys
Analyst in Science and Technology Policy

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.