Food and Agriculture Sector-Specific Plan

2015

FDA Food and Drug Administration

USDA

U.S. Department of Homeland Security

Table of Contents

Coordination Letter from Council Chairs

In 2003, the Federal Government designated the Food and Agriculture (FA) Sector as a critical infrastructure sector, recognizing its significant contribution to national security and the economy. Since then, the sector has successfully built public-private partnerships that improved information sharing, created forums to share best practices, and developed tools and exercises to improve incident response and recovery. The sector recognizes the value of partnership and continues to take steps to improve security and resilience.

2015 Sector-Specific Plan Update

As with the previous plans, this Food and Agriculture Sector-Specific Plan (SSP) represents a collaborative effort among the private sector; Federal, State, local, tribal, and territorial governments; and nongovernmental organizations to reduce critical infrastructure risk and increase universal sector resilience.

The Food and Agriculture Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) jointly developed the goals, priorities, and activities included in this SSP to reflect the overall strategic direction for the Food and Agriculture Sector. This SSP also illustrates the continued maturation of the Food and Agriculture Sector partnership and the progress made to address the sector's evolving risk, operating, and policy environments. The Sector's goals support the Joint National Priorities (JNP) developed in 2014 by the national council structures described in the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013).

Key Accomplishments

Since 2010, Food and Agriculture Sector partners in the public and private sectors have taken significant steps to reduce sector risk, improve coordination, and strengthen security and resilience capabilities:

- The Highly Pathogenic Avian Influenza (HPAI) Outbreak of 2015 was the largest animal health event in U.S. history. As a result, members from private industry, academia, State partners, the Federal Government, and other stakeholders worked together to improve response processes and capabilities by developing the Fall 2015 HPAI Preparedness and Response Plan;
- The Food and Agriculture Sector conducted the Cybersecurity Assessment & Risk Management Approach (CARMA) to critically examined cyber threats, consequences, and vulnerabilities from farm-to-fork to better identify and manage cyber risks;

- The Food Related Emergency Exercise Bundle (FREE-B) is a compilation of scenarios based on both intentional and unintentional food contamination events, and was designed to allow for multiple jurisdictions and organizations (medical community, private sector, law enforcement, first responder communities) to test their own plans, protocols, and procedures independently.

These achievements represent the effective and value-added collaboration among the Food and Agriculture SCC, GCC, and the co-Sector-Specific Agencies (SSAs), which are the U.S. Department of Agriculture (USDA) and Food and Drug Administration (FDA). Moreover, these achievements clearly demonstrate the sector's progress and collaborative approach to developing, prioritizing, and implementing effective security programs and resilience strategies.

In the same shared purpose that guided these actions and their support for the framework, concepts, and processes outlined in the NIPP 2013, Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21), Executive Order 13636: Improving Critical Infrastructure Cybersecurity (EO 13636), Presidential Policy Directive 8: National Preparedness (PPD-8), and Homeland Security Presidential Directive 9: Defense of U.S. Agriculture and Food (HSPD-9), Food and Agriculture Sector partners will continue their efforts to enhance the security and resilience of the Nation's critical infrastructure assets.

Sincerely,

LeeAnne Jackson
FA GCC Co-Chair
Food and Drug Administration

Josh Bornstein
FA GCC Co-Chair
U.S. Department of Agriculture

Clay Detlefsen
FA SCC Co-Chair
National Milk Producers Federation

Randy Gordon
FA SCC-Co-Chair
National Grain and Feed Association

Caitlin Durkovich
Assistant Secretary
Office of Infrastructure Protection
Department of Homeland Security

Executive Summary

Protecting the Nation's food and agricultural critical infrastructure is an important responsibility shared by Federal, State, local, tribal, and territorial governments and private sector partners. Interruption of operations within the sector could have a potentially devastating impact on the Nation's public health and economy. The security and resilience of infrastructure in the Food and Agriculture (FA) Sector requires all sector partners to undertake a number of integrated processes and procedures. As such, the FA Sector has developed a new set of sector priorities in this updated 2015 SSP that will help guide security and resilience efforts, inform partner decisions, reflect activities to enhance security and resilience, and improve risk management practices over the next four years. The achievement of the corresponding FA Sector goals will not only enhance security and resilience in the sector, but will also help measure the progress towards the NIPP 2013 goals, the JNP[1], and the National Preparedness Goal.

I. Introduction

The critical infrastructure of the United States, which includes assets, systems, and networks that provide vital services to the Nation, is essential to the Nation's security, economic vitality, and way of life. The protection of the Nation's critical infrastructure, therefore, is an essential part of the homeland security mission of making America safer, more secure, and more resilient from terrorist attacks and other natural and manmade hazards. In the context of the NIPP 2013[2], this includes actions to deter, mitigate, or neutralize the consequence, vulnerability, or threat associated with a terrorist attack or other incident. Protection can include a wide range of activities: safeguarding or shielding critical infrastructure assets, systems, networks, or their interconnecting links from exposure, injury, destruction, incapacitation, or exploitation; hardening facilities; building resilience and redundancy; and implementing cybersecurity measures. The NIPP 2013 provides the framework for the cooperation that is needed to develop, execute, and maintain a coordinated national effort that brings together all levels of government, the private sector, and international organizations.

The NIPP and its complementary SSPs provide a consistent, unified structure for integrating both existing and future critical infrastructure security and resilience efforts. It also provides the core processes and mechanisms to enable government and private sector partners to work together to implement critical infrastructure security and resilience initiatives.

[1] Joint National Priorities for Critical Infrastructure Security and Resilience (2014). http://www.dhs.gov/publication/joint-national-priorities. Accessed on 10/29/15.
[2] National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience (2013). http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience. Accessed on 10/29/15.

The purpose of the FA SSP is to guide and integrate the FA Sector's efforts to improve security and resilience, and to describe how the FA Sector contributes to national critical infrastructure security and resilience as set forth in PPD-21. As an annex to the NIPP 2013, this SSP tailors the strategic guidance provided in the NIPP 2013 to the unique operating conditions and risk landscape of the FA Sector. In addition to PPD-21, this SSP incorporates the guidance provided in EO 13636 and use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Aspects of this document also outline the FA Sector's efforts to support the National Preparedness Goal from PPD-8 and HSPD-9.

This SSP represents a collaborative effort among the private sector; State, local, tribal, and territorial (SLTT) governments; non-governmental organizations (NGOs); and Federal departments and agencies to work toward achieving shared goals and priorities to reduce risk to critical infrastructure. It also reflects the maturation of the FA Sector partnership and the progress made by the sector since the 2010 SSP to address the evolving risk, operating, and policy environments.

II. Sector Overview

A. Sector Profile

The FA Sector is composed of complex production, processing, and delivery systems and has the capacity to feed people and animals both within and beyond the boundaries of the United States. These food and agriculture systems are almost entirely under private ownership, operate in highly competitive global markets, strive to operate in harmony with the environment, and provide economic opportunities and an improved quality of life for American citizens and others worldwide. The FA Sector accounts for roughly one-fifth of the Nation's economic activity.[3] In 2012, total agricultural product sales amounted to $400 billion, with crops and livestock each accounting for roughly half the FA Sector.[4] One-fifth of U.S. agricultural production is exported, generating $144.1 billion in 2013, creating a positive trade balance of roughly $40 billion, and thereby fueling the U.S. economy.[5]

[3] Farm Service Agency, News Release No.0120.11, (2011). http://www.fsa.usda.gov/FSA/newsReleases?area=newsroom&subject=landing&topic=ner&newstype=newsrel&type=detail&item=nr_20110315_rel_0120.html. Accessed on 11/3/2015.
[4] National Agricultural Statistics Service, 2012 Census of Agriculture (2012). http://www.agcensus.usda.gov/Publications/2012/. Accessed on 04/13/2015.
[5] Foreign Agricultural Trade of the United States; Latest U.S. Agricultural Trade Data (2014). http://www.ers.usda.gov/data-products/foreign-agricultural-trade-of-the-united-states-(fatus)/latest-us-agricultural-trade-data.aspx#.U7GTbvldXIu. Accessed on 04/13/2015.

In 2014, there were more than 935,000 restaurants and institutional food service establishments and an estimated 114,000 supermarkets, grocery stores, and other food outlets. In addition, as of February 19, 2014, there were 81,575 Food and Drug Administration (FDA) registered domestic food facilities (warehouses, manufacturers, processors) and 115,753 FDA registered foreign food facilities. The United States Department of Agriculture (USDA) Food Safety and Inspection Service (FSIS) also regulates 6,755[6] establishments for meat, poultry, processed egg products, imported products, and voluntary inspection services. Additionally, the United States has roughly 2.1 million farms, encompassing 915 million acres of land. Collectively, American farms produce $212 billion in crop production. The top five cash-producing industries are cattle, poultry and eggs, corn, soybeans, and milk.[7]

Beyond domestic food production, the FA Sector also imports many ingredients and finished products, leading to a complex web of growers, processors, suppliers, transporters, distributors, and consumers. Changes in supply and demand fundamentals in different countries, logistical challenges, shifts in agricultural and import and export policy, and new developments in technology continually alter the competitive landscape of global agriculture and challenges facing American farmers. Further, through export trade and by providing food aid in disaster and poverty stricken areas around the world, U.S. agriculture has a positive global humanitarian impact and contributes to world food security.

[6] United States Department of Agriculture, Meat, Poultry and Egg Product Inspection Directory, (2015). http://www.fsis.usda.gov/wps/portal/fsis/topics/inspection/mpi-directory. Accessed on 3/5/15.
[7] National Agricultural Statistics Service, 2012 Census of Agriculture (2012). http://www.agcensus.usda.gov/Publications/2012/. Accessed on 04/13/2015.

Agriculture and Food

The Department of Homeland Security (DHS) has developed an Infrastructure Data Taxonomy (Appendix 6) to enable transparent and consistent communication regarding critical infrastructure between government and private sector partners. The FA Sector Taxonomy defines agriculture and food:

> *Agriculture comprises establishments primarily engaged in growing crops, raising animals, harvesting timber, and harvesting fish and other animals from a farm, ranch, or their natural habitats. Food establishments transform livestock and agricultural products into products for intermediate or final consumption. The industry groups are distinguished by the raw materials (generally of animal or vegetable origin) processed into food and beverage products. The food and beverage products manufactured in these establishments are typically sold to wholesalers or retailers for distribution to consumers.*

The FA Sector Taxonomy is divided into several categories:

- Supply
- Processing, Packaging, and Production
- Agricultural and Food Product Storage
- Agricultural and Food Product Transportation
- Agricultural and Food Processing Product Distribution
- Agricultural and Food Supporting Facilities
- Regulatory, Oversight, and Industry Organizations
- Other Agriculture and Food

Both USDA and the FDA, an agency within the Department of Health and Human Services (HHS), share regulatory responsibility for food. USDA is responsible for the regulation of meat, poultry, and processed egg products in accordance with the Federal Meat Inspection Act (FMIA), Poultry Products Inspection Act (PPIA), and Egg Products Inspection Act (EPIA). The FDA has responsibility for the remaining food products not under the regulatory authority of USDA. Food is defined in Section 201(f) of the Federal Food, Drug, and Cosmetic Act (FFDCA) as "(1) articles used for food or drink for man or other animals, (2) chewing gum, and (3) articles used for components of any such article."

The *National Strategy for Physical Protection of Critical Infrastructures and Key Assets* defines the FA Sector as "the supply chains for feed, animals, and animal products; crop production and the supply chains of seed, fertilizer, and other necessary related materials; and 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."[8] In general terms, the FA Sector comprises agricultural production and food systems that span the farm-to-fork continuum.

Food Defense, Food Safety, and Food Security

Food defense is the protection of food products from intentional contamination or adulteration where there is an intent to cause public health harm and/or economic disruption. *Food safety* addresses the accidental or unintentional contamination of food products. Although significant progress has been made in reducing unintentional contamination of food products, it remains a public health issue. The World Food Summit of 1996 defined *food security* as existing "when all people at all times have access to sufficient, safe, nutritious food to maintain a healthy and active life."[9] Three distinct variables are recognized as important to the achievement of food security: availability, access, and utilization.

B. Sector Risks

Risk, in the context of the NIPP 2013, is defined 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. Several threats and hazards are of significant concern to the FA Sector.

Food Contamination and Disruption (Accidental or Intentional)

- Contaminated food in the United States is estimated to be responsible for approximately 48 million illnesses, 128,000 hospitalizations, and 3,000 deaths, costing the Nation more than $14 billion a year in terms of medical care, lost productivity, chronic health problems, and deaths.[10]
- Violent extremists and terrorists consider America's agriculture and food production tempting targets and have indicated an interest in poisoning the food supply, which has great potential to cause costly economic losses in the supply chain for implicated foodstuffs, create public panic, and lead to a public health crisis with considerable mortality and morbidity.[11]
- A general disruption, such as an attack on a critical transportation or energy node, could impact the FA Sector even if the action was not targeting a FA Sector component.

[8] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (2003). http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf. Accessed on 10/29/15.
[9] Trade Reforms and Food Security (2003). http://www.fao.org/docrep/005/y4671e/y4671e06.htm. Accessed on 04/13/2015.
[10] Centers for Disease Control 2011 Estimates of Foodborne Illness in the United States (2011). http://www.cdc.gov/Features/dsFoodborneEstimates/. Accessed on 04/13/2015.
[11] FBI Law Enforcement Bulletin, Agroterrorism: Threats to America's Economy and Food Supply (2012). http://leb.fbi.gov/2012/february/agroterrorism-threats-to-americas-economy-and-food-supply. Accessed on 04/13/2015

Disease and Pests

- The accessibility of crops and animals on the farm and the extensive international and interstate movement of animals and products increase the FA Sector's vulnerability to rapidly spread disease.
- Modeling estimates and historical evidence demonstrate that a domestic outbreak of a foreign animal disease (FAD), such as Foot-and-Mouth Disease (FMD), would cost the United States billions of dollars due to loss of livestock, production, and international trade.

Severe Weather (i.e., Droughts, Floods, and Climate Variability)

- Natural hazards are a constant risk to the FA Sector and critically influence farm productivity.
- Climate change poses a major challenge to U.S. agriculture because of the critical dependence of the agricultural system on climate and the complex role that agriculture plays in rural and national social and economic systems.
- Weather and climate characteristics, such as temperature, precipitation, carbon dioxide, and water availability, directly impact the health and wellbeing of plants and livestock, as well as pasture and rangeland production.
- The harmful effects of severe weather coupled with global climate change are currently affecting U.S. water resources, agriculture, land resources, and biodiversity. This trend is expected to continue as production of all agricultural commodities will become more vulnerable to the direct impacts (e.g., changes in crop and livestock development and yield) and indirect impacts (e.g., increasing pressures from pests and pathogens) which result from changing climate conditions and extreme weather.[12]

Cybersecurity

Cyber threats and attack tools evolve rapidly as the cyberattacking community shows ingenuity. Most attacks can be blocked by continuously updated computer security programs. Such programs involve adherence to procedural safeguards for the system; an effective, continuously adaptive firewall; the application of intrusion detection and intrusion prevention systems for detecting, reporting, and preventing external threats to the network and information systems; surveillance programs for detecting insider threats; the continuous training of system users on proper security procedures; use of passwords resistant to hacker compromise; and related safeguards. Sector partners use cybersecurity measures as part of good business practices. Appendix A.2.5 describes FA Sector cybersecurity practices.

[12] U.S. National Climate Assessment Report (2014). http://nca2014.globalchange.gov/report. Accessed on 04/15/15.

One area of interest for the FA Sector is the use of Industrial Control Systems (ICS), such as Supervisory Control and Data Acquisition (SCADA), by many food production and processing facilities. With the vast majority of ICS developing to enhance connectivity and remote access, the vulnerability of these systems to cyber threats needs to be better understood. As the FA Sector becomes increasingly reliant on technology, the sector will continually revisit the issue of cybersecurity.

C. Critical Infrastructure Partners

PPD-21 designated USDA and HHS as the co-SSAs for the FA Sector. HHS has delegated this responsibility to FDA. The FA Sector comprises a set of private industries (owners and operators), represented by the Food and Agriculture Sector Coordinating Council (SCC), and government (Federal and SLTT) entities, represented by the Food and Agriculture Government Coordinating Council (GCC).

The SCC, which is a self-governing body representing the food and agriculture industry, provides a forum for members of the private sector to discuss infrastructure security and resilience issues among themselves or to communicate with the government through the GCC. The GCC, with representation from Federal and SLTT governments, is the public sector component of the food and agriculture public-private partnership framework. The objective of the GCC is to provide effective coordination of food and agriculture security and resilience strategies and activities, policy, and communication across government and between government and the sector to support the Nation's homeland security mission.

Security and resilience for the sector requires close collaboration between government and industry. Significant progress in the FA Sector on homeland security goals can only be accomplished through a partnership effort among all levels of government and critical infrastructure owners and operators. The FA Sector's main planning and coordination mechanisms for security and critical infrastructure partners are the SCC and the GCC. USDA and HHS, in concert with DHS, recognized the need for a mechanism to facilitate interaction with sector partners. The goal of establishing such a partnership is to leverage complementary resources in government and between government and industry to ensure a more robust, resilient, and secure sector.

The SCC Governance Principles and Operating Procedures and GCC charter with additional partner information and websites are available in appendices A.2.6 and A.2.7, respectively.

Sector-Specific Agencies

USDA and FDA share SSA responsibilities for the safety and defense of agriculture and food and have an obligation to provide leadership for sector infrastructure security and resilience activities, which include establishing information-sharing relationships and developing collaborative sector protection plans with sector critical infrastructure partners. USDA has responsibility for production agriculture and shares SSA responsibilities for food safety and defense with FDA. Specifically, FDA is responsible for the safety of 80 percent of all food consumed in the United States. The co-SSAs have been assigned responsibility for overseeing and coordinating security and resilience efforts, as well as disseminating guidance through the SSP.

USDA Leadership for SSA Responsibilities

At USDA, leadership for SSA responsibilities rests with the Office of Homeland Security and Emergency Coordination, which coordinates with all USDA agencies and offices to meet sector goals. USDA has statutory responsibilities to ensure that plants and animals are healthy and that the Nation's supply of meat, poultry, and processed egg products is safe, wholesome, and correctly labeled and packaged. USDA is also a research leader in human nutrition, animal and plant health protection, and new crop technologies that allow producers to grow more food and fiber using fewer resources. USDA helps to ensure open markets for U.S. agricultural products worldwide and, in cooperation with the United States Agency for International Development (USAID), provides international food assistance programs. USDA also provides a financial safety net to U.S. producers through market and disaster assistance programs and loans and a nutrition safety net for children and low-income people through the domestic nutrition assistance programs. Appendix A.2.1 summarizes USDA's key authorities. The nexus between these responsibilities and homeland security, specifically infrastructure security and resilience, lies in ensuring public health nationwide through a safe, plentiful, and affordable food supply while protecting the jobs that that produce it. Farming and ranching are the foundations of $1 trillion in food and fiber business, with nearly $60 billion in annual exports. They generate almost five percent of the Nation's Gross Domestic Product, as well as providing nearly 10 percent of the country's jobs.[13]

USDA has a long history of working with other governmental entities and private industry to support U.S. agriculture and food industries in ensuring the safety of our food supply. USDA agencies and offices are very active in outreach activities to accomplish its mission. The agencies help develop the productive and cooperative relationships of the large and diverse food and agriculture community through the creation of strategic alliances with stakeholders.

[13] USDA Economic Research Service Frequently Asked Questions (2014). www.ers.usda.gov/faqs. Accessed on 04/13/15.

FDA Leadership for SSA Responsibilities

Within HHS, SSA responsibilities reside with FDA's Office of Analytics and Outreach/Food Defense and Emergency Coordination Staff at the Center for Food Safety and Applied Nutrition, which coordinates across all FDA components to meet sector goals. FDA is responsible for protecting and promoting public health by, among other things, ensuring that the nation's food supply for human and animal consumption is safe, sanitary, wholesome, and properly labeled. FDA regulates $417 billion worth of domestic food and $49 billion worth of imported foods. FDA's responsibility in the food area generally covers all domestic and imported food, except meat, poultry, and processed eggs, which are primarily the responsibility of FSIS. FDA also regulates food, drugs, and devices for animals. This regulation takes place from the products' point of U.S. entry or processing, to their point of sale. In addition, roughly 935,000 restaurants and institutional food service establishments and an estimated 114,000 supermarkets, grocery stores, and other food outlets are regulated by State and local authorities. Appendix A.2.2 summarizes FDA's key authorities, and Appendix A.2.3 provides a summary table of USDA and FDA jurisdiction over food.

FDA works with its SLTT counterparts to further FDA's mission by funding contracts, grants, and cooperative agreements for States to conduct inspections on behalf of FDA and to build infrastructure and capacity in the funded programs. FDA provides training, guidance, and technical standards, including the model Food Code, the Manufactured Food Regulatory Program Standards, and the Voluntary National Retail Food Regulatory Program Standards, to regulatory and public health partners to support and promote uniform coverage of food establishments. FDA has also devoted significant time and resources to building a fully integrated national food safety system in collaboration with regulatory and public health partners.

FDA's Office of Regulatory Affairs (ORA) is the lead office for all agency field activities. ORA inspects regulated products and manufacturers, conducts sample analyses of regulated products, and reviews imported products offered for entry into the United States. Each of FDA's six major program areas (human drugs, devices, biologics, food and cosmetics, animal drugs and feeds, and tobacco products) has a complementary field component responsible for supporting the centers that ensure compliance with FDA regulations. ORA accomplishes this by inspecting regulated products and manufacturers, conducting sample analysis on regulated products, maintaining import data entry systems, and advising key officials on regulations and compliance-oriented matters that impact policy development and execution and long-range program goals.

Critical Infrastructure Owners and Operators, Including Private and Public Entities

Regional and national organizations that represent the owners and operators of agriculture establishments have regular communication with the SSAs. Through conference calls and

meetings, SSAs and agriculture stakeholders discuss security and resilience projects and initiatives underway by sector partners and collaborate on development and implementation of security and resilience strategies. The organizations representing agriculture stakeholders have the unique ability to call on their members to provide additional knowledge and technical expertise across the full range of critical infrastructure security and resilience activities and issues, making organizations a valuable asset for collaboration.

Department of Homeland Security

The FA Sector interacts with DHS through multiple components including the National Protection and Programs Directorate (NPPD), the Office of Health Affairs (OHA), and the Science and Technology Directorate (S&T).

The NPPD Office of Infrastructure Protection (IP), Sector Outreach and Programs Division has a key role in coordinating interagency, sector-wide, and cross-sector activities.

The NPPD Office of Cyber and Infrastructure Analysis (OCIA) identifies and assesses current and future threats to the Nation's physical and information infrastructure derived through various assessments and analyses of key risks to the Nation's critical infrastructure: terrorists; nation-states; malicious insiders; industrial accidents; lone-wolf assailants; and natural disasters. OCIA products are communicated to the sectors through the Homeland Security Information Network (HSIN).

The Office of Cybersecurity and Communications (CS&C) within NPPD leads the engagement and coordination of cybersecurity initiatives with government and industry partners. CS&C engages with the FA Sector and private sector owners and operators to support cyber preparedness within the sector and to ensure the security, resilience, and reliability of cyber and communications infrastructure.

The OHA Food, Agriculture, and Veterinary Defense (FAVD) Division provides oversight and management of DHS implementation of HSPD-9 by integrating efforts of other DHS components and coordinating those efforts with appropriate Federal departments and agencies, SLTT governments, and the private sector.

The OHA National Biosurveillance Integration Center (NBIC) consolidates data from all relevant surveillance systems that detect biological events of national concern impacting food and agriculture. NBIC analyzes the information, alerts member agencies, and coordinates with them in notifying State, local, and tribal governments. The OHA also has additional components which support State and local initiatives, response capacities, planning and exercising, and information exchange.

S&T was established by Congress in 2003 with the mission to deliver effective and innovative insight, methods, and solutions for the critical needs of the homeland security enterprise (HSE). As the Department's primary research and development (R&D) arm, S&T manages science and technology research, from development through transition, for the Department's operational components and the Nation's first responders. S&T's engineers, scientists, and researchers work closely with industry and academic partners to ensure R&D investments address the high-priority needs of today and the growing demands of the future. From border security and biological defense, to cybersecurity and explosives detection, S&T is at the forefront of integrating R&D across the public and private sectors and the international community.

By working directly with responders and component partners across the Nation, S&T strives to provide advanced capabilities and analytics to better prevent, respond to, and recover from all hazards and homeland security threats, including threats to the FA Sector. The S&T Chemical and Biological Defense Division supports threat assessments relevant to the FA Sector, the development of agricultural screening tools, the piloting of a veterinary passive surveillance system, and the management of the foreign animal vaccines and diagnostics research portfolio with the Plum Island Animal Disease Center and extramural researchers.

The majority of S&T investment in food defense is through the Office of University Programs (OUP) Centers of Excellence (COEs). The COEs are consortia of lead and partner academic institutions that operate using a unique research management approach in which researchers work alongside operational and decision-making HSE personnel and critical infrastructure sectors to apply science to enhance security and resilience capabilities. OUP's engagement with the homeland security community and the FA Sector has grown from a handful of active COE projects in 2004 to almost 250 in 2014 in response to rapidly increasing demand for university research, curriculum, students, facilities, and faculty advice.

The roles and responsibilities for DHS IP, OHA, and S&T include:

- NPPD-IP roles and responsibilities: According to PPD-21, DHS is responsible for coordinating the overall national effort to enhance the security and resilience of the critical infrastructure of the United States. In DHS, this overarching responsibility is delegated to IP.
- OHA-FAVD division roles and responsibilities: OHA-FAVD provides oversight and management of DHS implementation of HSPD-9 by integrating efforts of other DHS components and coordinating those efforts with appropriate Federal departments and agencies, SLTT governments, and the private sector.
- S&T roles and responsibilities: S&T administers a university-based system to enhance the Nation's homeland security. The Agricultural Defense Branch of the S&T Chemical and Biological Defense Division addresses countermeasure development and operates the COE and Minority Serving Institution programs, as well as the Workforce and Professional Development initiatives.

Other Government Departments and Agencies

The SSAs have interagency agreements with many other Federal and State agencies to delineate responsibilities for food and feed safety and animal and crop health. These agreements are the foundation for mapping relationships and delineating responsibilities among these Federal partners.

The SSAs maintain close communication with GCC Federal partners and other Federal agencies, including the Centers for Disease Control and Prevention (CDC), the Consumer Product Safety Commission, the Department of Commerce, the Department of Justice (DOJ), the Department of Transportation, the U.S. Environmental Protection Agency, the Federal Bureau of Investigation (FBI), and Federal Trade Commission. SSAs also receive information from other governmental security and intelligence agencies and guidance from the Office of Management and Budget (OMB) and the White House.

SLTT Governments

The SSAs work closely with SLTT entities. The program areas covered and jurisdictional lines can vary significantly, depending on each State or region in the United States. Primarily, State and local food protection and agriculture agencies have jurisdiction of the food supply at the retail and wholesale levels, including the receipt of agricultural products in the local jurisdiction. More than 3,000 SLTT agencies have primary responsibility to regulate the retail food and foodservice industries in the United States. They are responsible for the inspection and oversight of over one million food establishments—restaurants, grocery stores, vending machines, cafeterias, and other outlets in health care facilities, schools, and correctional facilities. State, tribal, territorial, and, in some cases, local animal and plant health programs also play an important role in the prevention, detection, and response to animal and plant diseases and pests.

International Organizations and Foreign Countries

Globalization is a fact of 21st century economic life. As a result, United States markets comprise a myriad of imported goods that consumers want and need.

The U.S. Department of State is the Federal Government's primary interlocutor with foreign governments and intergovernmental organizations. Accordingly, USDA, HHS, and other Federal agencies closely coordinate with Department of State for international cooperation on FA Sector initiatives, including, but not limited to, plant health, animal health, food safety, food defense, soil and water management, and market information systems. In addition, the United States participates in the international standard-setting programs of the International Plant Protection Convention, the World Organization for Animal Health (OIE), and the Codex Alimentarius to help

manage risks in the products flowing between the United States and our trading partners. The HHS Secretary's Operations Center and the USDA Operations Center receive alerts from the World Health Organization and OIE, such as International Health Regulations mandated notifications, about the occurrences of animal/plant diseases, emerging infectious diseases, etc. Generally, the alerts are provided in the form of emails to both 24-hour Operations Centers in Washington, DC.

Once the HHS and USDA Operations Centers receive an alert, the Watch Officers analyze and direct those emails to the appropriate agency emergency coordinator(s) or subject matter expert(s) for situational awareness and/or action.

Both HHS and USDA also receive incident-specific Situation/Spot Reports from the Department of State Operations Center on behalf of the Food and Agriculture Organization (FAO). These emails are also analyzed for content and internal USDA distribution.

III. Vision, Mission, Goals, and Priorities

A. Vision

The FA Sector is a prepared and resilient system of public and private sector partners engaged in risk-based decision-making and open communication with robust preparedness programs, threat prevention strategies, and vulnerability reduction activities with an all-hazards approach.

B. Mission

The mission of the FA Sector is to protect against a disruption anywhere in the food system that would pose a serious threat to public health, safety, welfare, or to the national economy.

C. Goals

Homeland security, particularly in the FA Sector, is not the responsibility of one department or agency in government, but, rather, is a partnership effort between all levels of government and private sector owners and operators. True gains in homeland security cannot occur without the support and action of the private sector.

Table 3-1: FA Sector Goals

GOAL	2015 2019 Sector Goals
Goal 1	Continue to promote the combined Federal, SLTT, and private sector capabilities to prevent, protect against, mitigate, respond to, and recover from manmade and natural disasters that threaten the national food and agriculture infrastructure.[14]
Goal 2	Improve sector situational awareness through enhanced intelligence communications and information sharing among all sector partners.
Goal 3	Assess all-hazards risks, including cybersecurity, to the FA Sector.
Goal 4	Support response and recovery at the sector level.
Goal 5	Improve analytical methods to bolster prevention and response efforts, as well as increase resilience in the FA Sector.

D. Priorities

These priorities support the furtherance of the FA Sector's goals:

Priority 1: Improve the ability to prevent, detect, and respond to animal and plant disease outbreaks and food contamination, whether naturally occurring or intentional, through the expansion of laboratory systems and qualified personnel.

- Links: SSP Goals 4 and 5; JNP 2 and 4; NIPP Goals 1, 2, and 3; NIPP Calls to Action 3, 4, 7, and 10; HSPD-9 Sections 8 (a, b, c), 10, 23, and 24; PPD-8 National Preparedness Goal; FDA Food Safety Modernization Act (FSMA) Section 109

Priority 2: Enhance and integrate existing information sharing approaches.

- Links: SSP Goal 2; JNP 3 and 5; NIPP Goal 4; NIPP Call to Action 5; HSPD-9 Section 19; FSMA Section 109

Priority 3: Raise awareness of and evaluate potential cyber risks, and encourage FA Sector members to use the NIST Cybersecurity Framework.

- Links: SSP Goal 3; JNP 1, 2, and 5; NIPP Goals 1, 2, 3, and 4; NIPP Calls to Action 2, 4, 6, and 8; HSPD-9 Sections 11 and 12; PPD-8 National Preparedness Goal

[14] Presidential Policy Directive 8: National Preparedness (2011). https://www.whitehouse.gov/blog/2011/10/07/ppd-8-announcing-national-preparedness-goal. Accessed on 10/29/15.

Priority 4: Continue to resolve decontamination and waste management related issues.

- Links: SSP Goals 1 and 4; JNP 2; NIPP Goal 3; NIPP Call to Action 8; HSPD-9 Sections 15and 16; FSMA Section 109 and 208

Priority 5: Engage all levels of the FA Sector in national planning efforts and goals.

- Links: SSP Goal 1; JNP 3 and 5; NIPP Goal 4; NIPP Call to Action 3, 4, 5, 6, 8, and 12; HSPD-9 Sections 11, 12, 13, 14, 15, 16, and 18 (a, b); PPD-8 National Preparedness Goal and National Planning Frameworks; FSMA Section 109

Several tables (table A.5-1, A.5-2, and A.5-3) are available in Appendix 5 that crosswalk the FA Sector's priorities to the JNP, NIPP Goals, and NIPP Calls to Action.

IV. Achieving Sector Goals

A. Risk Management

Identify Assets, Systems, and Networks

The FA Sector has a process to define, identify, collect, and store food and agriculture critical infrastructure systems' information that is pertinent to risk management. The focus of this identification is on systems in the FA Sector which, if damaged, would result in significant consequences on national economic security, national animal and public health and safety, public confidence, loss of life, or some combination of these adverse outcomes. There are a myriad of existing efforts on information collection practices and methodologies that support not only existing government regulation, but also oversight and private sector operations and logistical functions. In addition, there are multiple critical infrastructure identification and information collection efforts, challenges, as well as procedures for protecting sensitive and classified information used to guide critical infrastructure sector security and resilience decision-making activities.

To meet requirements of the NIPP 2013 for a strategic approach to critical infrastructure security and resilience, the FA Sector must understand its critical systems and subsystems. The FA Sector endeavors to establish methods and processes by which these systems can be evaluated, to assist in consideration of potential threats, to assess vulnerabilities, and to develop and implement protective measures and mitigation strategies. Also, it is perceived that these methods and

processes can help address R&D needs and measure successes. Protective efforts for the FA Sector must begin on the farm with inputs (e.g., fuel, fertilizer, livestock), move through processing and manufacturing (e.g., transportation, storage, transferring of supplies), and end with the consumer. Efforts must be made to identify and consider interdependencies and dependencies that exist with other sectors.

The critical asset information is collected through a DHS data call process and maintained on the DHS IP Gateway, a secure, controlled-access, web-based architecture that allows DHS critical infrastructure partners from all levels of government to access a wide variety of capabilities and analytical tools, and view Federal infrastructure data alongside that collected by SLTT partners. The IP Gateway enables critical infrastructure partners across DHS, the Federal Government, and the SLTT community to collect, manage, protect, and share authoritative infrastructure data between associated applications, and to conduct vulnerability assessments, assess risk, and respond to threats and incidents through a single integrated platform. While meeting diverse stakeholder needs, the IP Gateway provides a consistent vulnerability assessment and data collection methodology to support asset comparisons and robust analytics, enable compilation of data between applications, and maximize cross-government information sharing.

Components within the FA Sector and DHS collect, verify, update, and protect proprietary information for various uses. Data verification is a multifaceted process that varies according to the source of the data. Over time, data collection and verification processes are revised to ensure an even higher quality of data. Each year the existing data will be updated as part of data call processes.

The critical starting point for risk analysis is to define and identify critical infrastructure assets, systems, and networks and, in many cases, their associated functions. This definition and identification is the foundation for conducting a risk analysis, prioritizing infrastructure systems, and identifying the appropriate mix of protective programs and actions that will most effectively reduce risk

The FA Sector encourages partners to utilize the NIST Cybersecurity Framework in order to identify assets, systems, and networks. Released in February 2014, the Framework includes five core functions that express basic cybersecurity activities at a high-level with additional categories and subcategories that break them down into specific risk management activities. “Identify” is the first function which involves, among other things, identification of “data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes.”[15]

[15] Framework for Improving Critical Infrastructure Cybersecurity (2014). http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf. Accessed on 10/29/15.

Defining Information Parameters

As part of food safety responsibilities and food defense recommendations, the Federal Government and all SLTT partners must be able to identify and locate individual establishments, facilities, and firms from one end of the farm-to-table continuum to the other. For response and recovery efforts, the FA Sector needs the ability to identify those systems that might be affected by a terrorist attack, natural disaster, or manmade accident to know the status of the regulated facilities following all hazards. This represents an enormous challenge.

The FA Sector infrastructure, because of its unique, complex, broad-based, globally distributed, and highly integrated nature, is a system of systems (i.e., systems of individual assets that are closely dependent on each other). Because of its complexity, the FA Sector has struggled to define its most critical assets, systems, and networks. While the FA Sector understands its individual systems and basic interrelationships, the challenge has been in understanding and extrapolating data from the innumerable end points. Differences in the terminology used by sector partners contribute to the complexities to identify interdependencies across the farm-to-table continuum on regional, national, and international scales. The complexities and breadth of the FA Sector make data collection, verification, updating of critical infrastructure information difficult.

Despite the aforementioned challenges, when determining and assessing risks, the FA Sector categorizes critical infrastructure by individual facilities or systems according to the process utilized by DHS. By taking an individual facility-based or a systematic approach to identifying critical assets through the annual National Critical Infrastructure Prioritization Program (NCIPP), it is possible to identify the food types and facilities most at risk for compromise and determine the most vulnerable points in the farm-to-table continuum. As new developments in the definition of FA Sector infrastructure information occur, the SSAs will capture and provide this information in the FA Sector Annual Report (SAR).

The FA Sector relies on DHS and the Intelligence Community (IC) to provide threat information to assist with the definition, identification, collection, verification, and updating of critical infrastructure information. The FA Sector leadership, in collaboration with States, will use pertinent threat intelligence to determine and document the most critical elements, systems, and subsystems in the FA Sector.

In the FA Sector, no overarching plan for the definition and identification of all critical infrastructure information exists; however, a tremendous amount of information is collected across the spectrum of sector regulatory, enforcement, and oversight activities. Similarly, laboratory-related assets, systems, and networks, while performing these day-to-day activities, are also producing, analyzing, and comparing infrastructure information.

Collecting Sector Critical Infrastructure Information

PPD-21 directs the Secretary of DHS to lead efforts to reduce the Nation's vulnerability to terrorism and deny the use of infrastructure as a weapon by developing, coordinating, integrating, and implementing plans and programs that identify, catalog, prioritize, and protect critical infrastructure in cooperation with all levels of government and private sector entities.

As previously stated, the diverse and complex nature of the FA Sector poses a challenge to the task of determining which sector assets are critical. The critical infrastructure information collection effort includes an outreach component so that sector partners in industry and SLTT governments understand the purpose and criteria of the information needed. Through the DHS annual NCIPP data call, the SSAs have worked with SLTT governments and private sector partners in an attempt to collect the critical infrastructure information for the FA Sector.

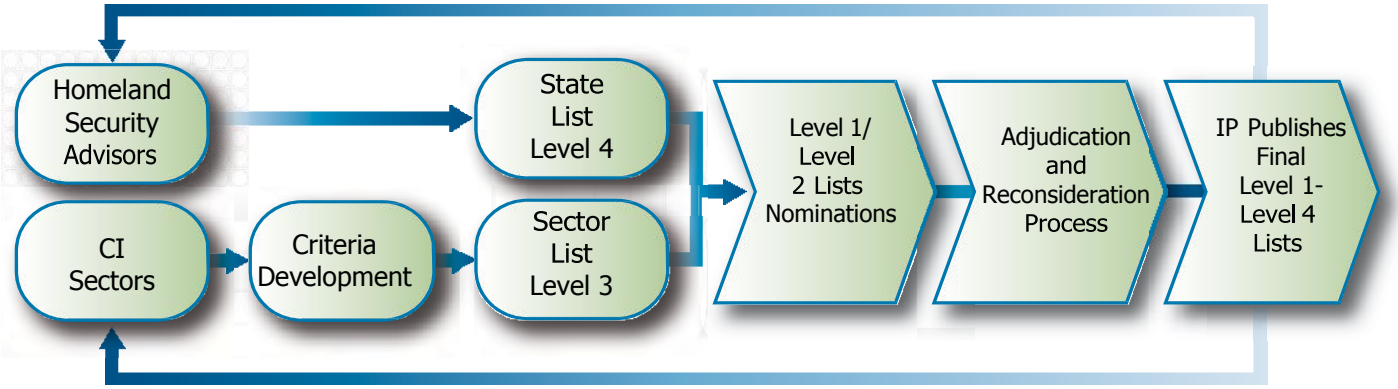
Data Call Process

In accordance with the 9/11 Commission Act, DHS is the lead coordinator in the national effort to identify and prioritize the Nation's critical infrastructure. DHS executes this responsibility through the NCIPP, which includes data calls to identify domestic infrastructure that would, if disrupted, cause national or regional catastrophic effects. The Level 1 and Level 2 lists inform State homeland security and other grant programs. They are used during incidents to prioritize Federal, State, and local response and recovery efforts. The Critical Foreign Dependencies Initiative, which identifies similar critical infrastructure outside the United States, also helps to identify and prioritize critical infrastructure.

DHS maintains four levels of critical infrastructure for this purpose based on the following criteria:

- **Level 1 (All Sectors):** Infrastructure that, if disrupted, could result in very significant consequences to human life, the economy, national security, or property.
- **Level 2 (Agriculture and Food Sector-Specific):** Infrastructure that, if disrupted, could result in significant consequences to international, national, or regional economic stability, national security, or property.
- **Level 3 (All Sectors):** Infrastructure that does not meet Level 1 or Level 2 criteria but is recognized by Sector leadership to be so important to the Nation as to warrant special consideration.
- **Level 4 (All Sectors):** Infrastructure submitted by each state or territory utilizing their own criteria.

Figure 5-1: The DHS Data Call Process



The main purpose of all four lists (Level 1–Level 4) is to provide a common basis that DHS and critical infrastructure sector partners can use to develop and implement important critical infrastructure security and resilience programs and initiatives. The lists will continue to be used to focus planning, foster coordination, and support effective incident management, response, and restoration activities by DHS, Federal and SLTT governments, and private sector partners.

Protected Critical Infrastructure Information

One of the key components for collecting infrastructure information is the ability to preserve the confidentiality of the information submitted by the private sector, of which much is proprietary. Although the private sector would like to share sensitive business or security information with its Federal or State critical infrastructure partners, it may hesitate to do so because of concerns about protecting the information from disclosure. Thus, a level of trust is needed that the information will be used only for the stated purposes and that it will be protected from public release. The DHS Protected Critical Infrastructure Information (PCII) program offers a mechanism for industry to share and the government to protect sensitive business and security information.[16] The SSAs will continue working with DHS IP Infrastructure Information Collection Division to provide PCII-specific guidance to sector partners as necessary.

[16] Information submitted to satisfy the requirements of the Critical Infrastructure Information Act of 2002 is protected from public disclosure under the Freedom of Information Act, State and local disclosure laws, and use in civil litigation. More information about the PCII program is available at http://www.dhs.gov/pcii. Accessed on 04/13/15.

Verifying Critical Infrastructure Information

Programmatic-based information collected from sources regulated by the SSAs can be easily verified. Because of the complexities and diversity of the FA Sector, however, an overarching formal process to verify critical infrastructure information provided to the SSAs through the data calls has not yet been identified. Infrastructure information collected by the SSAs for regulatory or other mission-related purposes is verified by data quality control; validated through onsite meetings; and verified through producers and members of industry, other Federal Government agencies, and the States. Although this verification work is part of regulatory requirements and other efforts, it does contribute to the larger critical infrastructure data verification process.

DHS IP Protective Security Advisors verify critical infrastructure information provided through DHS data calls while performing individual site visits at the actual facilities located across the United States, working closely with SLTT governments and private sector partners.

Updating Critical Infrastructure Information

The FA Sector endeavors to establish a formal process to update and verify critical infrastructure information. As new developments in the updating and verification process occur, SSAs will capture and provide this information in the SAR.

Sector Dependencies and Interdependencies

The FA Sector has numerous dependencies (one-directional reliance of an asset, system, or network) and interdependencies (mutually reliant relationship between entities) with other sectors. The nature and extent of these dependencies and interdependencies increase the risks borne by the FA Sector, based on the function and role of those dependencies and interdependencies, and may lead to future integrations and collaborations to assist with the identification and fortification of existing vulnerabilities.

As part of a larger effort examining chemical, biological, and radiological events impacting the critical infrastructure workforce, the National Infrastructure Advisory Council (NIAC) was charged with examining interdependencies between and among the critical infrastructure sectors in the wake of a pandemic. In its 2008 report, Chemical, Biological, and Radiological Events and the Critical Infrastructure Workforce, Final Report and Recommendations by the Council, NIAC said:

> "the complexity of interdependencies among [critical infrastructure]… sectors cannot be understated. Furthermore, as business operations change and criticalities evolve, interdependencies shift in importance. The Study Group believes that these interdependencies must be mapped clearly so sectors are better able to protect their critical assets in the wake of a severe pandemic influenza and better prepared to defend themselves against potential cascading failures across sectors." [17]

The NIAC report makes numerous other references to interdependencies and the need for additional study and research to adequately capture and describe these relationships. Specifically, the report states that the key findings of the survey included:

- **Interdependencies across critical infrastructure sectors** are exceptionally high in a biological event and must be fully understood. The interdependent relationships most often cited were for the basic municipal and other infrastructure support requirements, including energy, information technology (IT), communications, and water.
- **Subtle interdependencies between critical goods and services and the critical infrastructure worker,** including basic physical security requirements, financial services for businesses and workers, and food and healthcare to sustain workers and their families, are no less important than the direct interdependencies.
- **Supply chain interdependencies,** specifically the essential role transportation plays as a bridge between all levels of the supply and distribution chain, are yet another venue to be further studied and understood.

All of the aforementioned types of interdependencies are predicated on the fact that the critical infrastructure workers rely on the full spectrum of the FA Sector.

[17] Chemical, Biological, and Radiological Events and the Critical Infrastructure Workforce, Final Report and Recommendations by the Council (2008). http://www.dhs.gov/publication/niac-chemical-biological-radiological-final-report. Accessed on 10/29/15.

Example: Dependencies on Water, Transportation Systems, and Chemical Sectors

As an example of a dependency, the FA Sector is dependent on the *Water Sector* to provide a continuous supply of potable water and adequate wastewater facilities. Water is necessary for processing facilities, livestock production, and crop irrigation at the farm level, where water sources often include rivers, reservoirs, lakes, and groundwater. In addition, food and ingredient manufacturing relies on water, especially municipal water and wastewater systems, for processing. A water shortage would limit the ability of farmers to irrigate crops, but the Water Sector would not be directly impacted by a large scale FA Sector disruption.

Similarly, the *Transportation Systems Sector* provides the means for delivering inputs to the farm, including items such as seeds, seed stock, fertilizer, and feed required for agricultural production. The FA Sector is then dependent on the Transportation Systems Sector to deliver the agricultural products to processing facilities, distribution facilities and retailers, and, finally, to the consumer.

The FA Sector relies on fertilizers and pesticides supplied by the *Chemical Sector* for the production of economical and plentiful agricultural products.

Example: Interdependencies with the Commercial Facilities and Financial Services Sectors

The *Commercial Facilities Sector* could be significantly impacted and experience losses in revenue by a large scale disruption of the FA Sector, specifically at the retail level. The FA Sector relies on Commercial Facilities to sell product.

The *Financial Services Sector* could face catastrophic damage via the agriculture commodity exchanges in the event of an attack or failure of within the FA Sector. The Financial Services Sector provides the financial backbone for food and agriculture business in the United States.

The FA Sector, in collaboration with other sectors and DHS, seeks to illustrate and further examine these dependencies and interdependencies. Some benefit could be realized by beginning to address overlaps and interdependencies to aid in future planning, integration, and coordination not only to eliminate redundancy in efforts, but also to create a synergistic relationship in which each sector can benefit from its respective overlaps. These overlaps could identify the existing strengths and potential vulnerabilities that could be in need of improvement or resiliency strategies.

Assess Risks

Risk, as defined by the NIPP 2013, is derived from an equation that incorporates consequence, vulnerability, and threat. The FA Sector typically focuses on systems and networks in addition to individual assets when conducting a risk assessment.

The NIPP risk management framework calls for critical infrastructure partners to assess risk from any scenario as a function of consequence, vulnerability, and threat, as defined below. As stated in the NIPP, "it is important to think of risk as influenced by the nature and magnitude of a threat (T), the vulnerabilities to that threat (V), and the consequences that could result (C)."[18] The NIPP also contains criteria designed to help comprehend consequence, vulnerability, and threat.

$$R = f(C,V,T)$$

- **Consequence (C) Analysis:** Estimates the potential, animal health, public health, and economic impacts that a successful attack could cause;
- **Vulnerability (V) Assessment:** Identifies weaknesses in an asset design, implementation, or operation that can be exploited by an adversary; and
- **Threat (T) Analysis:** Estimates the likelihood that a particular target, or type of target, will be selected for attack, and is based on the intent and capability of an adversary.

Risk Assessment in the Sector

Historically, risk assessments have been used to help focus limited resources where they can have the greatest impact. Risk assessments of food safety are used to determine the quantitative or qualitative value of risk attributed to exposure to an identified food contaminated with a biological or chemical hazard. Conversely, vulnerability assessments identify, quantify, and prioritize vulnerabilities in an asset, system, or network, and those assessments are an especially useful

[18] National Infrastructure Protection Plan (2009). http://www.dhs.gov/publication/nipp-2009-partnering-enhance-protection-resiliency. Accessed on 11/17/15.

approach to prioritize actions to mitigate identified vulnerabilities. HSPD-9 directs USDA, HHS, and DHS to expand and continue to conduct vulnerability assessments of the FA Sector and update these assessments every two years. Private sector owners and operators have conducted vulnerability assessments because it is in the best interests of their companies.

The FA Sector has identified and uses various resources to identify and determine each component of risk: consequence, vulnerability, and threat.

The first component of risk, consequence, is assessed through the accumulation of reportable data (e.g., illness and death and economic impact). Both USDA and FDA have mechanisms to monitor adverse events. The information is aggregated to produce a clear picture of the consequence for each type of disaster.

The CARVER+Shock methodology—which stands for Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability, + Shock—was designed to identify vulnerabilities in assets, systems, and networks that comprise the FA Sector by encompassing the consequences and threats. The vulnerability assessments conducted by the SSAs have looked at systems and networks instead of particular assets. Vulnerability assessments help SSAs identify the products of highest concern, threat agents likely to be used, points in the production process where intentional contamination is most likely to occur, laboratory testing and research needs, and potential countermeasures.

The National Counterterrorism Center (NCTC) is the lead entity in determining the final component of risk, threat. All FA Sector threats deemed credible by law enforcement agencies are investigated further with assistance from FA Sector partners. As previously discussed, the FA Sector relies on threat information provided by DHS and the IC to determine the criticality of known risks. The FA Sector will prioritize and address the most critical risks through working groups, which will survey sector membership on what resources are available and develop a plan of action to enhance the security and resilience of the identified critical assets. Any proposed and implemented protective programs will be continually assessed to determine their efficacy in addressing potential threats. Dependent on resource and budget availabilities, the remaining identified risks will be managed by the FA Sector.

In addition, DHS developed the Threat and Hazard Identification and Risk Assessment (THIRA) as a four step common risk assessment process that helps government and private sector partners (i.e., any entity receiving federal grants for preparedness activities) understand the risks within their community and estimate capability requirements. The THIRA process helps communities understand how to best manage and plan for the greatest risks within the full spectrum of threats and hazards it faces.

THIRA's four step process is composed of:

1. Identify threats and hazards of concern
2. Give the threats and hazards context
3. Establish capability targets
4. Apply the results

The outputs of this process inform a variety of emergency management efforts, including emergency operations planning, mutual aid agreements, and hazard mitigation planning.

The critical infrastructure within the FA Sector is largely privately owned and operated, which requires a community approach to risk assessments as outlined by THIRA. Collaboration and information sharing by government and private sector entities, as highlighted in the Strategic Partnership Program Agroterrorism (SPPA) initiative and new efforts, such as FSIS's cybersecurity vulnerability assessment initiative, are the key to securing the vast and open network of systems that comprise the FA Sector.

Assessing Vulnerabilities

To depict the relationship and contents of this section the following terms, excerpted directly from the NIPP, illustrate the relationship between the opportunity (vulnerability) and outcome (consequence) of an attack in the FA Sector.

Vulnerability is defined as a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. In calculating risk of an intentional hazard, the common measure of vulnerability is the likelihood that an attack is successful, if it is attempted.

Many of the FA Sector's interdependent systems defy traditional security practices because they are not brick-and-mortar entities, like buildings, bridges, or dams. Instead, they are open areas (e.g., farms, ranches, or livestock transport areas) and complex systems that span the globe. Many of these systems face natural threats, including livestock and crop diseases and foodborne pathogens. Because of these variables, it may not be feasible to prevent the introduction of threat agents; therefore, the FA Sector has acknowledged the importance of early awareness or surveillance by veterinarians, agriculture producers, and nationally coordinated disease surveillance programs that have the ability to target different threat agents in its systems.

The interdependent relationships within and among other sectors present numerous vulnerabilities that could be problematic for the sustained and contained provision of services within each sector. Thus, to accurately portray the risk of these interdependencies in the FA Sector, one needs to clearly identify these points of dependence on critical partner sectors, and subsequently coordinate with those SSAs to address, mitigate, and fortify these vulnerabilities. Several examples of these interdependencies are described in the Sector Overview section.

CARVER+Shock

The FA Sector has utilized CARVER+Shock to fulfill this dual role of vulnerability and consequence assessment. CARVER+Shock is an offensive targeting prioritization tool adapted from the military version (CARVER) for use in the food industry. The tool can be used to assess the vulnerabilities within a system or infrastructure to an attack. It allows the user to think like an attacker to identify the most attractive targets for an attack. By conducting a CARVER+Shock assessment of a food production facility or process, the user can determine the most vulnerable points in their infrastructure and focus resources on protecting the most susceptible points in their system.[19]

Biosurveillance

In addition to traditional public health surveillance conducted by FDA and FSIS, and in partnership with SLTT officials and the CDC, USDA and HHS interface and collaborate with NBIC to monitor and coordinate surveillance information on both unintentional and intentional food and animal health incidents. This program allows agencies to identify trends, patterns, and anomalies in data, including outbreak data and vulnerabilities in food safety systems. Collected data is consolidated and analyzed, which allows for the early detection of unintentional and intentional food, animal, and plant health incidents. Intelligence information generated from active biosurveillance will provide for the early detection of threats, guide responses to events, and allow for information sharing among agencies.

Additionally, USDA and S&T have partnered with the COE for Zoonotic and Animal Disease Defense (ZADD), led by the Institute for Infectious Animal Diseases (IIAD) at Texas A&M University, to develop a first-of-its-kind Enhanced Passive Surveillance (EPS) capability, which utilizes web-based or iPad applications to record location and occurrence of syndromic animal health data in near-real time and compiles it into a dashboard to monitor syndromic prevalence. The EPS project supports electronic capture of observational health data from animal herds under the care of private practitioners and livestock managers. If specific clinical disease case definitions are met, the project will support an associated lab workup. Participating practitioners, managers, State and Federal animal health officials will be provided user-appropriate data access for analysis and reporting of aggregated user-shared data. This three year R&D project began in November 2013 following successful pilots initiated in the previous year. The EPS project is focused on the data confidentiality issue as it is a voluntary data submission process. The project is also trying to address interoperability within the animal health community (domestic and wild) and between health communities (Animal, Human, and Environment). If implemented with good coverage, the information generated through this project can help mitigate potential spread of diseases by having an electronic collaboration within the practicing community.

[19] Additional information on CARVER+Shock is available at http://www.fda.gov/food/fooddefense/fooddefenseprograms/ucm376791.htm.

Federal Perspective

HSPD-9 requires USDA and FDA to conduct vulnerability assessments of the FA Sector and to update them every two years. Including the effort under the SPPA Initiative, conducted from 2005-2008, over 50 vulnerability assessments have been conducted on a variety of food and agricultural products, processes, or commodities under the regulatory authority of the FDA and USDA. In addition to the SPPA assessments, USDA has conducted more than 30 vulnerability assessments and updates that include, but are not limited to, products and factors such as deli meats, establishment size, ground beef, hot dogs, imported food products, liquid eggs, ready-to-eat meals, National School Lunch Program, ready-to-eat chicken, threat agents, transportation, and water used in food. FDA conducted an additional 18 vulnerability assessments and updated 16 of the original assessments conducted under the SPPA Initiative. These assessments helped to form the foundation of the food defense program within the U.S. and to enhance communication and collaboration among industry, government, law enforcement, and academia.

FDA and USDA have also been active partners in the risk assessment efforts led by DHS (Biological Terrorism Risk Assessment, Chemical Terrorism Risk Assessment, Radiological/Nuclear Terrorism Risk Assessment, and the Integrated Terrorism Risk Assessment) to ensure that food and agriculture interests are appropriately included.

Typically, vulnerability assessments conducted by the Federal government are not site- or company-specific; but focus on high-level operational or systems processes or a particular industry. Risk assessment results are shared with Agency leadership to request resources to support protective programs developed to address the identified risks.

In the cybersecurity arena, the FA Sector acknowledges the potential damaging consequences of a successful attack and maintains an ongoing assessment of sector specific threats. A potential area of concern is the use of ICS by food production and processing facilities. The most commonly found ICSs in industries, such as the FA Sector, include SCADA systems, distributed control systems, and Programmable Logic Controllers. These control systems help to regulate and manage the various and dispersed assets in the production process. Traditionally, ICSs were self-contained and isolated, running on specially developed software and hardware. More recently, an observed trend is the replacement of traditional ICSs with readily available and cost efficient Internet Protocol systems. These new systems encourage corporate connectivity and allow for remote access capabilities, which fall in line with best practices for industry efficiency and innovation. However, the increased connectivity of ICSs present an opportunity for unwanted intrusions with harmful consequences. Some possible threats the FA Sector may face, include:[20]

[20] Guide to Supervisory Control and Data Acquisition and Industrial Control Systems Security (2006). http://www.dhs.gov/sites/default/files/publications/csd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf. Accessed on 04-13-15.

- Blocked or delayed flow of information through ICS networks
- Unauthorized changes to instructions, commands, or alarm thresholds that could potentially damage, disable, or shutdown equipment
- Dissemination of inaccurate information to system operators, to either disguise unauthorized changes or to initiate inappropriate actions
- Modification of ICS software or settings, or infection of ICS software with malware
- Interference with the operation of safety systems

In order to facilitate the cyber assessment of the FA Sector, the sector is engaging with CS&C to access the available resources and to identify appropriate approaches and methodologies to conduct cyber vulnerability assessments. Some of the identified resources include:

- Cybersecurity Assessment & Risk Management Approach (CARMA)
- Cyber Security Evaluation Program and Cyber Resilience Review process
- Cyber Infrastructure Survey Tool and Cyber Security Evaluation Tool

Utilizing CARMA, the FA Sector will be able to identify, assess, and manage national or regional risks to the cyber-dependent critical infrastructure that are shared by FA Sector stakeholders and mitigate cyber risks through the use of identified best practices based upon input from subject matter experts. The FA Sector, led by FSIS, will also use aspects of the Cyber Resilience Reviews with individual stakeholders participating in the cyber assessment to provide a bottom-up sector perspective to the assessment that will complement CARMA's top-down sector approach.

The FA Sector develops awareness of operational resilience and encourages the management of cyber risks by supporting the conduct of Cyber Resilience Reviews offered through the Cyber Security Evaluation Program.

Another way the FA Sector encourages the development of cybersecurity capabilities is through the use of the Critical Infrastructure Cyber Community (C^3) Voluntary Program. The FA Sector educates critical infrastructure owners within the FA Sector about the program and recommends participation in order to strengthen cybersecurity within the sector.

Additionally, DHS offers tools to support FA Sector identification of sector cyber infrastructure and to evaluate the cybersecurity of networks within the FA Sector. The FA Sector can use the Cyber Infrastructure Survey Tool to assess the essential cybersecurity practices to support cybersecurity planning efforts. The Cyber Security Evaluation Tool assists critical infrastructure owners and operators to assess their network infrastructure and components related to their ICS or SCADA systems and helps them to identify where to focus efforts to improve cybersecurity.

EO 13636: Improving Critical Infrastructure Cybersecurity was released in February 2013 and directed federal offices to take several actions that affect the FA Sector:

- The NIST was directed to develop a Cybersecurity Framework that "shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible."[21] This Cybersecurity Framework was released in February 2014.
- DHS, specifically CS&C, was directed to work with Sector-Specific Agencies to create a Voluntary Critical Infrastructure Cybersecurity Program "to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities."[22]
- "Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the SCCs to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments."[23]

In response to these initiatives, the FA Sector will encourage the use of the NIST Cybersecurity Framework in coordination with the C^3 Voluntary Program. The FA Sector will educate critical infrastructure owners within the FA Sector about cyber risk management, the Framework, and resources available through the C^3 Voluntary Program and recommend activities in order to strengthen cybersecurity within the FA Sector.

SLTT Perspective

Several states and local governments have used risk assessments to identify food and agriculture-related vulnerabilities in their jurisdictions. Some have partnered with the Federal Government and industry to conduct assessments. State assessments may be more narrowly focused on particular industries in the State. The protection of this information varies by State law.

Private Sector Perspective

Private industry assessments are typically focused on a particular company, site, or a process in a specific company or site. Many private companies are choosing to assess their operations to determine how to best use their resources. These assessments, while not classified, are carefully guarded and rarely shared with government partners because they identify specific vulnerabilities in a company, site, or process point. A number of private firms, industries, related trade organizations, and private voluntary organizations have demonstrated a general willingness to work with government partners to conduct vulnerability assessments, as demonstrated during the

[21] Executive Order 13636: Improving Critical Infrastructure Cybersecurity (2013). https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. Accessed on 10/29/15.
[22] Executive Order 13636: Improving Critical Infrastructure Cybersecurity (2013). https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. Accessed on 10/29/15.
[23] Executive Order 13636: Improving Critical Infrastructure Cybersecurity (2013). https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. Accessed on 10/29/15.

SPPA initiative. Time constraints, concerns about exposing vulnerabilities, sharing proprietary information, and assessment-related expenses limit the ability of some firms to participate in vulnerability assessments.

Assessing Threats

Threat is defined in the 2013 NIPP as a natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and property. Risk calculation considers the threat of an intentional hazard as the likelihood of an attack being attempted by an adversary. For other hazards, threat is generally estimated as the likelihood that a hazard will manifest itself. In the case of terrorist attacks, the threat likelihood is estimated based on the intent and capability of the adversary.

The Federal Government, under the NIPP, is responsible for providing threat information for each sector. Threat information is available from various sources; however, DHS, law enforcement, and the IC are the primary sources.

Risk and threat assessments help prioritize resources to protect the FA Sector's infrastructure. The SSAs continue to work with OCIA to obtain threat information. For risk and threat assessments, the following types of threat products will be used:

- **Common Threat Scenarios:** Present possible terrorist methods that could be used in attacks against U.S. infrastructure. DHS developed these scenarios from analyses of terrorist intentions and capabilities and plans to update them as required.
- **General Threat Environment:** Assess sector-specific threats that consider known terrorist threat information. General threat environment assessments also include longer term strategic assessments and trend analyses of the evolving threat to the sector's critical infrastructure.
- **Specific Threat Information:** Use real-time intelligence streams and infrastructure-specific information to assess threats. Products will drive short-term protective measures to mitigate risk and contribute to the general threat environment and common threat scenario products produced by DHS.

Federal Perspective

SSAs continue to partner with the IC. Both FDA's Office of Criminal Investigations (OCI) and USDA's Office of the Inspector General (OIG) maintain a presence at NCTC. All threat information, foreign and domestic, that is directed against the United States or its interests is received and evaluated by the NCTC. First, threat information determined to be credible is passed to the SSAs to be used as necessary to protect the lives and wellbeing of the public. Second, threat information determined to be both credible and actionable is referred to the appropriate law enforcement

agency for action and passed to the SSAs. Operational law enforcement information would not be passed unless failure to do so would result in harm to the public.

The appropriate law enforcement agency in most cases would be one of the FBI Joint Terrorism Task Forces made up of agents from various Federal, State, and local law enforcement agencies. Both OCI and OIG participate on the National Joint Terrorism Task Force. OCI and OIG agents would have a major role in any threat or criminal investigation involving FDA- and USDA-regulated products. These agents would also be responsible for the coordination of FDA and USDA assets in the criminal investigation (e.g., subject matter experts, laboratory support).

SLTT Perspective

States and private sector representatives work with local law enforcement to ensure that available threat information is shared with the appropriate Federal officials. The FBI's weapons of mass destruction (WMD) coordinators play an important role in collaborating with the States and the private sector to maintain awareness of threats.

Assessing Consequences

> The DHS Risk Lexicon defines consequence as the effect of an event, incident, or occurrence. Consequence reflects the level, duration, and nature of the loss resulting from the incident.

The Consumer Complaint Monitoring System (CCMS) is an electronic database used to record, triage, coordinate, and track all consumer complaints reported to FSIS. FSIS maintains CCMS as an integral part of its bio-defense strategy to track and assess all potential threats and consequence of incidents affecting FSIS-regulated products. FSIS Directive 5610.1[24] describes the purpose, activities, and maintenance of the CCMS system. For purposes of the CCMS, a consumer complaint is any complaint reported to FSIS that is initiated by a consumer, or by someone on behalf of a consumer, that is directly related to a meat, poultry, or processed egg product. Generally, product complaints allege illness, injury, foreign object, allergic reaction, misbranding, economic adulteration, and inferior quality.

All complaints are triaged to determine if further investigation is warranted and by whom, or to close the complaint. Results of complaint triage and subsequent actions taken are reported to consumers and establishments, unless the case is an ongoing criminal investigation. Special

[24] FSIS Directive: Procedures to Implement the Consumer Complaint Monitoring System (2005). http://www.fsis.usda.gov/OPPDE/rdad/FSISDirectives/5610.1.pdf. Accessed on 10/29/15.

attention is provided to certain non-routine cases, and may lead to the activation of the FSIS Emergency Management Committee, if appropriate.

Similarly, FDA uses the Center for Food Safety and Applied Nutrition (CFSAN) Adverse Event Reporting System (CAERS) Tool, which provides a single system for tracking and evaluating adverse events and consumer complaints received by FDA concerning food, dietary supplements, and cosmetics. Congressional funding allowed for the development of a basic system for report collection, which includes a document management system that permits data entry and report redaction and allows scanned reports to be seen at reviewers' computer stations.

CAERS also sends a notification to manufacturers of a product that receives an adverse event report. Consumers, health professionals, or industry staff contact FDA district offices or FDA MedWatch[25] to report adverse events or product problems, and these reports are forwarded to CAERS for entry in the system. This tool provides CFSAN with a search capability for adverse event data. CAERS aids FDA in identifying new and emerging food, dietary supplement, and cosmetic-related public health problems.

If feasible and appropriate, CAERS information indicating a potential food defense incident may be shared with affected industry sectors and the FA Sector HSIN. Collection of post-market reports about CFSAN-regulated products improves FDA's ability to identify and analyze food product-related risks.

Reportable Food Registry (RFR)[26] is an electronic portal for industry to report reasonable probability that an article of food will cause serious adverse health consequences. RFR helps FDA better protect public health by tracking patterns of adulteration in food. RFR supports FDA efforts to target limited inspection resources to protect the public health.

Information Sharing and Protection

One of the NIPP 2013 goals is to improve situational awareness through enhanced intelligence communication and information sharing, within and across sectors, to enable risk-informed decision-making. Although there are no sector requirements for information sharing, members recognize the importance of maintaining an open line of communication between all stakeholders.

[25] MedWatch: The FDA Safety Information and Adverse Event Reporting Program (2015). http://www.fda.gov/Safety/MedWatch/default.htm. Accessed on 10/29/15.
[26] Reportable Food Registry for Industry (2014). http://www.fda.gov/food/complianceenforcement/rfr/default.htm. Accessed on 04/13/15.

Information Sharing

As in most partnerships, effective communication is essential to success. The SCC and GCC have acknowledged that effective communication requires two-way, routine information sharing and discussion. To ensure a sustainable information sharing process, the Information Sharing Working Group (ISWG) was formed with members from the public and private sectors to assess capability gaps and to develop solutions in various topic areas, to include:

- HSIN-Food and Agriculture (FA) Membership
- Testing of Emergency Notification System for FA Sector Members
- Previously developed information sharing processes
- Re-development of HSIN-FA webpage
- Cataloging of existing information sharing efforts

Additionally, the Food Protection and Defense Institute (FPDI), with private sector and association partners, recognized that threat information sharing between the public and private entities within the FA Sector, if properly managed, could be one of the Nation's most powerful tools to combat FA Sector risks. FPDI is currently conducting research in three areas to facilitate improved information sharing among the individuals, agencies, and companies.

- National Association of County and City Health Officials (NACCHO) is conducting an 18-month mixed methodological study to help improve FA Sector security by identifying gaps and understanding inhibitors to optimal bidirectional threat information sharing within the FA Sector. The results of research activities will be used to develop a set of recommendations for improving and sustaining bidirectional information sharing between FA Sector public and private stakeholders in prioritized areas and relating to specific incidents, threats, consequences, and vulnerabilities. Final dissemination of results is expected to be in spring 2016. NACCHO is also leading two other ongoing projects that similarly examine gaps in the information sharing processes within the FA Sector between private-to-private and government-to-government.
- The Association of State & Territorial Health Officials is conducting a systematic review and legal analysis of existing State laws and regulations relating to State and Territorial Health Agencies (STHAs) authority to protect non-public information from public disclosure. In addition, a survey will be issued to all 50 States and territories followed by key informant interviews to gain insight into the interpretation of current laws impacting the disclosure of food safety and defense related information. Case studies and other practical resources for STHAs will be developed and posted online to facilitate better intragovernment information sharing.
- FPDI researchers are investigating the legal barriers, perceptions, and company policies that allow or prohibit regular and proactively shared information on food system issues and/or disruptions. A series of interviews with key personnel from national and multi-

national companies will be conducted. The outcome of this research will provide new knowledge gained on industry procedural and technical information-sharing requirements to help inform the private sector and regulators in determining information-sharing procedures.

The following systems and networks are used for information sharing and distribution in the FA Sector.

HSIN

As the SCC and GCC mature and can process and act on information, additional means of communication are necessary for ensuring real-time, robust information sharing. The GCC and the SCC use HSIN as a platform for communications and information sharing.

The HSIN-FA portal is a communications portal used by approved private sector entities and individuals, as well as Federal, State, and local government employees. The HSIN-FA portal has a number of different areas or subportals with various restrictions about who can and cannot access them.

When HSIN-FA users log in, they see the main or common area page. Depending on access rights and interests, users may obtain access to additional areas in the portal. Beyond the main page, HSIN-FA is divided in two major areas, SCC and GCC.

The SCC area, including any subportals, is for the exclusive use and benefit of private sector users. Control of the SCC area resides exclusively with the private sector. Any material posted in or otherwise conveyed through the SCC areas is the property of the private sector and is not considered government information.

Federal, State, and local government agencies and their affiliated users and employees control and maintain the GCC portion of HSIN-FA. These users may grant private sector access at the sole discretion of the GCC Co-Chairs. The GCC creates and eliminates subportals under the main GCC areas and posts information to those areas as it deems appropriate.

Sharing of Threat Information

FA Sector partners rely mainly on DHS as the source for threat-related information. To educate FA Sector partners concerning potential threats, OCIA provides unclassified alerts, warnings, and information bulletins that are distributed through the GCC and SCC.

Additionally, the National Cybersecurity and Communications Integration Center shares information among the public and private sectors to provide greater understanding of cybersecurity and communications situation awareness of vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

Governmental sector partners also participate in the Joint Terrorism Task Force program, where the FBI shares information with local law enforcement and other sector partners concerning specific threat information and investigations involving terrorism (FBI is the lead agency).

To further formalize the mechanism for the communication of threat information and to strengthen the FBI's relationship with the FA Sector, the FBI directed its field offices to establish formal agroterrorism working groups in its jurisdiction. These working groups will enhance the relationships between Federal partners by bringing together representatives from all entities involved in proactive prevention and awareness, intelligence, investigative response, and crisis management. USDA and FDA do maintain relationships with the FBI and other law enforcement and intelligence agencies.

FoodSHIELD

FoodSHIELD provides a web-based information sharing platform for Federal regulatory agencies, laboratories, State and Local government entities, military branches, and academics involved in protecting and defending the food supply and responding to foodborne disease outbreaks and safety concerns. It was initiated by a USDA Cooperative State Research, Education, and Extension Service (CSREES) grant and is predominantly operated and maintained by leveraging infrastructure obtained through portions of R&D funding combined with contributions from FDA, USDA, and DHS to FPDI.

FoodSHIELD has proven to be essential in enhancing collaboration and communication in the Sector, particularly as the Sector works toward full compliance with PPD-21 and HSPD-9. There are many features available and/or used by USDA to increase information sharing. Food and Agriculture specific applications include the Economically Motivated Adulteration database, the Laboratory Directory of Integrated Resources, the Food and Agriculture Research Database, and the Farm Toolkit.

Information Protection

Often, the information used by FA Sector partners to effectively manage risk and secure the Nation's critical infrastructure will contain sensitive security information, sensitive business and proprietary information, or classified information. The latter is protected by EO 12958, as amended under EO 13292. One challenge of classifying important sector security information, however, is the inability to easily share it with key State and industry sector partners. It would benefit FA Sector security if more State and industry officials had security clearances.

Information protection is a significant concern for partners that share sensitive business or proprietary information that cannot be classified for protection. The Federal leadership for the FA

Sector—USDA and FDA, with DHS—takes the need to protect this information seriously and will do so to the maximum extent allowed by law.

Chief among the tools used by the FA Sector to protect business-sensitive or proprietary information is the DHS PCII Program, developed according to the Critical Infrastructure Information (CII) Act of 2002, which requires creation of a Critical Infrastructure Information Program to receive sensitive and proprietary critical infrastructure information. If the PCII Program satisfies the requirements of the CII Act, information designated as PCII will be protected from public disclosure to the maximum extent permitted by law.

The rules governing the PCII Program are located in Title 6, Part 29 of the Code of Federal Regulations (CFR). General information is available on the PCII Program website, including instructions on how to properly submit information in compliance with the program. Final regulation also permits submissions to Federal SSAs.

In addition to the PCII Program, other regulations may affect the privacy of data submitted to a Federal sector partner. For example, under the Freedom of Information Act (FOIA), the public may request access to information the government possesses; however, FOIA contains an exemption for trade secrets and confidential business information, and this exemption should cover information submitted regarding private facility security.

Some States also face challenges in collecting critical infrastructure information because their laws do not protect such information from public release. This varies from State to State and may preclude sharing sensitive information with the States.

Prioritize Infrastructure

After potential risks are identified, the FA Sector can then attempt to prioritize its infrastructure. While other sectors look to their SSAs or to the GCC/SCC partnership to conduct the prioritization, the diffuse nature of the FA Sector makes any universal authority for prioritization impractical and ill-advised. Ultimately, prioritization for the FA Sector needs to be scenario-dependent and the responsibility of FA Sector partners and private sector owners and operators, with assistance from Federal and SLTT governments.

As with any other industry, the owners and operators of facilities and components of the FA Sector use many computer-based systems for information sharing and threat evaluation. ICS and SCADA systems are routine components in food processing. However, not all production and distribution of food is computer (cyber) dependent. Thus, many owners and operators have not considered cyber threats to be a critical risk; therefore, cybersecurity continues to be an area for improvement with the FA Sector because physical security risks have traditionally received

priority in attention and resources over cyber risks. This application of resources is continuously examined and adjusted by FA Sector leadership.

National Prioritization

The current prioritization process determines criticality according to consequence-related metrics. The FA Sector is in the process of collecting data and refining risk assessments so that the prioritization can move from a consequence-based metrics approach to a risk-based approach (inclusive of consequence). Because the FA Sector has focused its risk assessments on food and agriculture systems and not specific assets and networks, the results will reflect that approach. The likely outcome is a ranking with systems at the top and networks and assets below, which is a reflection of the FA Sector's composition. Outcomes of the process will be validated by the Infrastructure Data Warehouse so that the SSAs can work directly with owners and operators to develop and implement appropriate protective measures. It is the expectation of the SSAs that the prioritizations will be reviewed annually as part of the SAR development process.

As with other sectors that use the non-specific asset type configuration (i.e., Communications and Transportation Systems Sectors), food and agriculture systems become more critical depending on the type of incident or event, location, and the specific effects on end users in the impacted area. To determine which assets, systems, and networks are most critical during situational impact analyses, systems-based evaluations of the impact on the FA Sector consider several criteria:

- Duration of disruption (i.e., assuming return to operations is feasible);
- Complete destruction of facilities (i.e., return to operations is not feasible);
- Relationship of the system to the overall commodity being produced (i.e., loss of acreage of corn fields versus loss of entire specific product);
- Ability of adjacent and nearby facilities to adequately compensate for the loss of production or service;
- Financial markets; and
- Critical infrastructure supporting response and recovery.

During incidents, industry and government representatives can work together through the National Response Coordination Center to identify priorities for recovery and restoration. Ideally, the fully mature process can use the criteria listed above to generate priorities based on specific scenarios. With sufficient resources, a library will be created so that the criticality of a particular system will be known before the onset of a disaster because a model was previously generated. In the absence of a fully mature prioritization system, the FA Sector will continue to identify criticality on an as-needed basis with coordination and input from all relevant partners. As of this plan's publication, resources are not in place to support such a robust national prioritization.

State Prioritization

The process of State prioritization is attempted through participation in the DHS OCIA data calls. States have not uniformly responded to the request for assets meeting the criteria used, and, consequently, DHS has removed many of the submitted assets from the list because of this lack of uniformity in the submissions. The FA Sector is working toward improving the submission process so that critical food and agriculture assets will qualify as Level 2 assets, which can increase the likelihood of eligibility for DHS Homeland Security grant funding. To augment the Level 2 asset lists, DHS has asked each State to compile a State list (Level 4). The State list criteria are to be determined by each State. State-specific criteria are important because criticality can be determined in a number of potential ways, and the justifications provided will help explain these differences. Some States may define a critical facility as one that employs the greatest number of people; another State may prioritize a facility that generates the most income for the community; while a third State may say that the facility with the widest distribution of food is most important. The SSA, in coordination with DHS, will act as a central repository of the State lists. Collectively, the State lists will provide a picture of the FA Sector's prioritized assets that adequately acknowledges regional variability and decentralized systems. States that participate in the annual data call do so with the intention of not only submitting critical assets and systems for consideration for potential grant funding, but also helping to accurately depict the risk borne by the FA Sector in their State.

Research and Development

The FA Sector has developed four R&D priorities for the next three to five years. SSAs will continue to focus R&D efforts in these directions as resources permit. At the time of this SSP publication, these priorities aligned with the Critical Infrastructure Security and Resilience National R&D Priorities (CISR National R&D Plan).[27]

The CISR National R&D Plan, required by PPD-21, was released in February 2015. It presents five overarching critical infrastructure security and resilience national R&D priority areas that are intended to inform R&D investments, promote innovation, and guide research across the critical infrastructure community.

[27] Critical Infrastructure Security and Resilience National Research and Development Plan Final Report and Recommendations (2014). http://www.dhs.gov/publication/niac-cisr-national-rd-plan-final-report. Accessed on 10/29/15.

Critical Infrastructure Security and Resilience National R&D Priority Areas

1. Develop the foundational understanding of critical infrastructure systems and systems dynamics.
2. Develop integrated and scalable risk assessment and management approaches.
3. Develop integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure.
4. Harness the power of data sciences to create unified, integrated situational awareness and to understand consequences of action.
5. Build a crosscutting culture of critical infrastructure security and resilience R&D collaboration.

FA Sector R&D Priorities

1. *Cybersecurity*: Assess cybersecurity risks to the FA Sector.
2. *Analytical*: Identify requirements for characterization and detection of threat agents and prioritize the capability gaps.
3. *Risk Analyses*: Assess the vulnerability of the FA supply chain to natural and manmade threats and hazards.
4. *Information Sharing*: Assess current protocols for information sharing, identify communication gaps and barriers, and develop processes to support optimal information sharing between FA Sector partners.

More information on FA Sector Academia and Research Centers is available in Appendix 3.

B. Critical Infrastructure and National Preparedness

Develop and Implement Protective Programs and Resiliency Strategies

Because criticality is the function of an event and can only be determined as the needs of a response are identified, the FA Sector has developed strong relationships among the partners to ensure that all systems are resilient. One component of the resilience strategy is to encourage the implementation of protective strategies or risk mitigation activities (RMAs). The protective program development and implementation process builds on the FA Sector's goals.

The FA Sector has a mature set of RMAs, protective measures, and partnerships that include various government initiatives, as well as initiatives developed and implemented by industry partners. Government-sponsored protective programs enable industry to better work together to address issues that normally would not be addressed collectively because of competition. This document is strategic in its focus and is not intended to illustrate response activities; therefore, numerous examples of protective programs are provided and referenced to help FA Sector partners prepare for and respond to an incident impacting the Sector.

Overview of Sector Protective Programs and Resiliency Strategies

In 2010, the FA Sector used an informal process to compile a list (non-prioritized) of key RMAs from FA Sector leadership. To capture the complexity of the FA Sector, the RMAs submitted were groupings of activities rather than individual programs. The FA Sector will continue to review and pursue these RMAs within the context of the new, overarching priorities for the FA Sector:

- **Priority 1**: Improve the ability to prevent, detect, and respond to animal and plant disease outbreaks and food contamination, whether naturally occurring or intentional, through the expansion of laboratory systems and qualified personnel.
- **Priority 2**: Enhance and integrate existing information sharing approaches.
- **Priority 3**: Raise awareness of and evaluate potential cyber risks, and encourage FA Sector members to use the NIST Cybersecurity Framework.
- **Priority 4**: Continue to resolve livestock disposal and related decontamination issues.
- **Priority 5**: Engage all levels of the FA Sector in national planning efforts and goals.

A list of the FA Sector's ongoing and proposed RMAs, while not intended to prioritize in a formal manner, is available in Appendix 4.

Protective Program and Resiliency Strategy Implementation

At the Federal level, USDA's implementation and maintenance of protective programs focus on protecting farm animals and crops from disease outbreaks and pest infestations; protecting the supply of meat, poultry, and processed egg products; enhancing agricultural and food safety research and laboratory facilities; and improving emergency preparedness and response. Within USDA, individual agencies determine responsible staff for implementing and maintaining their programs within budgetary constraints. FDA issues regulations in accordance with congressional mandates and produces guidance documents for the private sector that contain suggested food defense practices and control measures according to applicable government regulations. The private sector, to varying degrees, may voluntarily implement applicable countermeasures.

Additionally, the FA Sector supports and enhances the integration of security and resilience activities through continued collaboration and open communication between public and private sector partners. By creating a common platform for information sharing, Federal and SLTT agencies and private stakeholders are able to come to consensus on feasible, economically viable security and resilience goals and programs. Ideally, industry owners and operators identify and share risk concerns that are encountered on a daily basis, which, when coupled with threat information generated by government agencies, results in comprehensive protective programs and resiliency strategies. The SSAs are also heavily engaged with the National Security Council on Domestic Resilience Group and critical infrastructure security and resilience activities. This effort brings together the interagency to develop policies across government that increases the security and resilience of all sectors.

The FA Sector recognizes the gravity of a successful cyberattack and has made cybersecurity a priority for the Sector. The NIST developed the Cybersecurity Framework to assist critical infrastructure sectors and organizations mitigate and manage their cyber risks. The FA Sector understands the increasing interconnectivity between cyber and physical security and recognizes the need for critical infrastructure owners and operators to implement integrated cyber and physical security measures to enhance security and resilience within the FA Sector. In order to support security and resilience activities, the FA Sector encourages its membership to use the Framework to strengthen critical infrastructure cybersecurity and promotes participation in the C^3 Voluntary Program established by DHS in February 2014. The FA Sector supports C^3 Voluntary Program participation by providing C^3 resources and various engagement opportunities. In addition, the FA Sector hosts the C^3 Voluntary Program at its Joint Sector Meetings to increase visibility of the program to members. The FA Sector also provides its membership information about other available resources and programs to promote security and resilience of physical and cyber infrastructure, such as the DHS Cyber Resilience Review process and CARMA, among others.

While the development of protective programs and resiliency strategies is determined through a consensus-based process between the GCC and SCC, final implementation of protective programs is determined by industry's ability to fund, incorporate, train staff, and adhere to the characteristics of the programs and strategies.

V. Measuring Effectiveness

A. Sector Activities

In pursuing the advancement of critical infrastructure and resilience, the FA Sector is committed to and engaged in a wide range of security and resilience activities. The FA Sector has

accomplished and will continue to pursue a range of activities to advance efforts that support presidential directives and EOs and align with the NIPP goals, FA Sector goals, and NIST Cybersecurity Framework performance goals. Some notable programs and plans underway at the time of plan publication are noted below.

In 2014, the DHS Federal Emergency Management Agency (FEMA) Region VII led planning efforts for the development of the Food, Agriculture, and Veterinary (FAV) Incident Response Annex. The FAV Annex is FEMA's support to USDA and HHS during an event that impacts Region VII. The sole intent of this plan/annex is to provide support in a coordinated, rapid, whole-community response to any FAV incident requiring Federal support under the National Response Framework. The FAV Annex will be used by Region VII during an incident to support the Federal Lead Agency to assist with containment, eradication, or control of a FAV emergency. The collaborative planning team consisted of over 500 people from 18 Federal agencies, 9 Tribal nations, 4 states, 37 NGOs, and 56 private sector partners.

DHS, with the support of USDA/Animal and Plant Health Inspection Service (APHIS), State Animal Health Officials, the DHS COEs, IIAD, and cooperating segments of the livestock industry, piloted the EPS project as a new biosurveillance tool to obtain early detection of animal disease outbreaks and gain better situational awareness of national herd health. This program entails real-time, mobile reporting of animal incidents and illnesses by voluntary industry partners who provide valuable data that can be leveraged to enhance animal health resiliency and mitigation of disease outbreaks. Once fully operational, EPS will be a tool that helps reduce risk in the FA Sector by providing information that will support early detection and mitigation efforts.

The 2014 USDA Climate Change Adaptation Plan integrated input from 11 USDA subagencies and offices. The Adaptation Plan provides a vulnerability assessment, reviews the elements of USDA's mission that are at risk from climate change, and provides actions and steps being taken to build resilience to climate change specifically in response to EO 13653: Preparing the United States for the Impacts of Climate Change. In addition, the plan advances efforts to integrate climate change adaptation planning into the actions of the Federal Government through the President's Climate Action Plan (PCAP), other executive orders, and USDA departmental policies. The PCAP identifies approximately 72 actions that the Federal Government should take. USDA is participating wholly or in coordination with other agencies in 19 actions including identifying vulnerabilities to climate change, maintaining agricultural sustainability, managing drought and leading efforts to address climate change through international negotiations.

Seven regional climate hubs deliver science-based tools, strategies, and practical information to farmers, ranchers, and forest landowners within each region of the United States to support decision-making related to climate change. These hubs maintain and strengthen agricultural production, natural resource management, and rural economic development under increasing climate variability. The hubs build capacity within USDA to deliver information and guidance on

technologies and risk management practices at regional and local scales. USDA subagencies are developing plans to educate their employees and their stakeholders and accommodate expected changes associated with climate change. Also, partnerships between scientists and land managers are being strengthened to improve the focus of research and technology to address current and emerging science and information needs. [28]

Additionally, the FA Sector is beginning efforts to examine how to improve communications with tribal members and enhance their engagement in GCC activities. The active involvement of tribal partners in the FA Sector is critical to ensuring a secure and resilient critical infrastructure system due to the focus on agriculture in many tribal communities.

The FA Sector, through the collaborative efforts of USDA, FDA, SLTT partners, industry, and academia, produced educational and engagement resources for industry partners to facilitate the development and adoption of food defense plans. A functional food defense plan is one that is documented, implemented, tested, reviewed, and maintained. Both USDA and FDA offer guidance, tools, and/or templates for development of food defense plans to food processing establishments and food facilities, respectively, to assist in the development of these plans. Outreach initiatives by FDA are conducted in accordance with the authorities provided by FSMA for protecting against the intentional adulteration of food. USDA continues to engage in direct outreach, particularly to very small establishments to improve awareness and adoption of functional food defense plans.

As previously mentioned, cybersecurity has become a high priority for the FA Sector in enhancing the security and resilience of FA Sector critical infrastructure. In March 2013, FSIS convened a focus group to discuss potential cyber vulnerabilities associated with the production and distribution of FSIS-regulated products. The focus group included representatives from government, industry, and academia and found that it was important to consider the entire supply chain to understand reliance on cyber technology and potential vulnerabilities. Based on the focus group's recommendation, FA Sector leadership decided to invest heavily in a cybersecurity vulnerability assessment led by FSIS and conducted in close collaboration with FDA, DHS, and industry. The cybersecurity vulnerability assessment will leverage the NIST Cybersecurity Framework and the C^3 Voluntary Program to improve understanding of cybersecurity risks and vulnerabilities in the FA Sector and ultimately inform countermeasures and guidance. While this vulnerability assessment will focus on the actual food processing facilities regulated by FSIS, the FA Sector plans to complete a CARMA assessment simultaneously. The CARMA assessment will inform the FSIS vulnerability assessment, as well as serve as a tool for the broader FA Sector by identifying and informing on Sector-specific cyber risks. The FA Sector plans to complete a CARMA assessment in 2015.

[28] USDA Climate Change Adaptation Plan (2014). http://www.usda.gov/oce/climate_change/adaptation/adaptation_plan.htm Accessed on 10/29/15.

In the private sector, industry leaders continue to proactively address threats to their industries to ensure the public health through a physical and economic access to sufficient food to meet their dietary needs for a productive and healthy life, while protecting the jobs of those who produce that food. The National Cattlemen's Beef Association, with the assistance of USDA/APHIS, is currently taking steps to develop a business continuity and resiliency and response plan, "Secure Beef," for FMD. This plan will be similar to other Secure Food Supply (SFS) plans in addressing the movement of animals and products during an FAD emerging disease incident, such as FMD. Other comparable plans include the Secure Milk Supply, Secure Pork Supply, Secure Egg Supply, and Secure Broiler Supply.

The U.S. pork industry has secured funding and is developing a Swine Health Information Center that will focus on identification and mitigation of nonregulatory emerging disease threats that could affect swine health and the security and affordability of the food supply.

B. Measurement Approach

The intent of measuring the effectiveness of FA Sector activities is to gauge the progress in enhancing the Sector's overall security and resilience over the next four years. Currently, the FA Sector lacks an overarching, all-encompassing mechanism to measure and evaluate the effectiveness of theme-based RMAs and their supporting programs, activities, and initiatives. In order to create a holistic view of the FA Sector's security and resilience stance, it is the goal of the FA Sector to take a segmented approach by evaluating the progress of individual protective programs and strategies.

Process for Measuring Effectiveness

USDA and FDA agency-specific program managers collect metrics as needed for their own requirements and use for budgetary needs, managing their workforce, and adhering to reporting requirements established by law.

Obtaining performance measurements from non-Federal partners remains challenging. Few States, industries, and other partners are willing to share programmatic data for several reasons (e.g., security of warehousing the data, potential uses of the information, and undertaking the reporting burden). These programs are normally run over the course of many years, and the metrics requested by different entities are not consistent over the long-term. Therefore, hesitation in reporting continues until a more concrete, coordinated, and overarching metrics strategy can be achieved.

Additionally, the final implementation of protective programs for critical assets is dependent on industry's ability to fund, incorporate, and adhere to the requirements of the programs. This

variability contributes to the presence of an inconsistent resilience posture across the FA Sector, which further complicates the ability to measure the FA Sector's overall security and resiliency. The FA Sector will continue to work to identify metrics and performance measurements to report on the status of the protection and resiliency of the FA Sector.

However, some planned metrics for measurement of protective programs previously mentioned include:

- The FA Sector will collaborate with DHS and APHIS-Veterinary Services (VS) to measure the progress of the EPS project by assessing participation and population coverage metrics by species and by area (state and county levels). Over time it is expected that population coverage will expand as a percentage of National Agricultural Statistics Service population estimates for each species covered. Once EPS is a self-sustaining program, its efficacy can be monitored by assessing how many potential outbreak incidents per species were identified and investigated via syndromic surveillance signals over a specified time period.
- The FA Sector will assess the progress of its various information sharing projects by evaluating the identified capability gaps or needs, suggested solutions, and programs developed to implement said solutions. A specific measurement of progress for the FA Sector's utilization of HSIN is to determine the number of HSIN account holders in the FA Sector, the number of postings to HSIN-FA, and an overall HSIN usage trend.
- FSIS began measuring the status of industry's voluntary adoption of food defense plans via annual surveys in 2006. Each year, the survey is issued to Inspection Program Personnel within FSIS-regulated meat and poultry slaughter and processing establishments, egg product plants, and official import inspection establishments to determine if establishments have a functional food defense plan. The ninth annual food defense plan survey was completed in July and August 2014. Overall, 84% of all establishments responding to the survey have a functional food defense plan (up from 83% in Fiscal Year (FY) 2013). The tenth annual food defense plan survey will be conducted in June 2015.
- USDA/VS will measure the progress of industry's voluntary adoption of SFS plans.
- The FA Sector will assess the progress and mark the completion of its initial cybersecurity vulnerability assessments (CARMA and the examination of FSIS-regulated facilities) with reports that detail the final findings of the assessments. The reports for both VAs are expected to be finalized by the fall of 2015.

C. Continuous Improvement

Exercises and Incidents

The FA Sector participates in exercises in order to test and measure the efficacy of current security and resilience procedures. The outcome of each simulation or scenario provides feedback on how

to enhance the protection of critical infrastructure. A couple of notable examples are included below.

In FY2015, the FA Sector will be participating in a national level exercise in South Carolina called Southern Exposure. This exercise will be focusing on mitigation programs, as well as response and recovery activities following an incident at the nuclear power plant resulting in the release of radiological material into the surrounding area.

The Food Related Emergency Exercise Bundle (FREE-B) is a compilation of scenarios based on both intentional and unintentional food contamination events. It is designed with the intention of assisting government regulatory and public health agencies in assessing existing food emergency response plans, protocols, and procedures that may be in place or are in the process of being revised or even developed. The FREE-B is designed to allow for multiple jurisdictions and organizations (medical community, private sector, law enforcement, first responder communities) to 'play' with the host agency, or, quite simply, for an individual agency to test their own plans, protocols, and procedures independently.

FDA developed FREE-B in cooperation with CDC, APHIS, and FSIS. Additionally, numerous subject matter experts participated in various rounds of reviews and refinement of the FREE-B.

The FREE-B is currently a set of five scenarios, each of which contains a Facilitator's Guide, a Lead Planner's guide, and a Situation Manual. Additional scenarios are under development for release in 2015.

Additionally, the FA Sector participates in multi-jurisdictional and cross-sector after action report processes for real-world events and works to implement action items as identified.

VI. Appendices

Appendix 1. Acronyms and Glossary of Terms

A.1.1 List of Acronyms and Abbreviations

ACIO	Associate Chief Information Officer
AMS	Agricultural Marketing Service
APHIS	Animal and Plant Health Inspection Service
C³	Critical Infrastructure Cyber Community
CAERS	CFSAN Adverse Event Reporting System
CARMA	Cybersecurity Assessment & Risk Management Approach
CARVER + Shock	Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability, + Shock
CCMS	Consumer Complaint Monitoring System
CDC	Centers for Disease Control and Prevention
CEEZAD	Center of Excellence in Emerging and Zoonotic Animal Diseases
CFR	Code of Federal Regulations
CFSAN	Center for Food Safety and Applied Nutrition
CIO	Chief Information Officer
CIPAC	Critical Infrastructure Partnership Advisory Council
COE	Centers of Excellence
CS&C	Office of Cybersecurity and Communications
CSREES	Cooperative State Research, Education, and Extension Service
DFO	Designated Federal Officer
DHS	Department of Homeland Security
DOJ	Department of Justice
EDEN	Extension Disaster Education Network
EO	Executive Order
EPIA	Egg Products Inspection Act

EPS	Enhanced Passive Surveillance
FA	Food and Agriculture
FAD	Foreign Animal Disease
FAV	Food, Agriculture, and Veterinary
FAVD	Food, Agriculture, and Veterinary Defense
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FFDCA	Federal Food, Drug, and Cosmetic Act
FISMA	Federal Information Security Management Act
FMD	Foot-and-Mouth Disease
FMIA	Federal Meat Inspection Act
FNS	Food and Nutrition Service
FOIA	Freedom of Information Act
FPDI	Food Protection and Defense Institute
FREE-B	Food Related Emergency Exercise Bundle
FSIS	Food Safety and Inspection Service
FSMA	Food Safety Modernization Act
FY	Fiscal Year
GCC	Government Coordinating Council
HHS	Department of Health and Human Services
HSE	Homeland Security Enterprise
HSIN	Homeland Security Information Network
HSIN–FA	Homeland Security Information Network–Food and Agriculture Sector
HSPD	Homeland Security Presidential Directive
IC	Intelligence Community
ICS	Industrial Control Systems
IIAD	Institute for Infectious Animal Diseases
IFPTI	International Food Protection Training Institute
IP	Office of Infrastructure Protection

ISWG	Information Sharing Working Group
IT	Information Technology
JIFSAN	Joint Institute for Food Safety and Applied Nutrition
JNP	Joint National Priorities
NACCHO	National Association of County and City Health Officials
NAICS	North American Industry Classification System
NBIC	National Biosurveillance Integration Center
NCBRT	National Center for Biomedical Research and Training
NCIPP	National Critical Infrastructure Prioritization Program
NCTC	National Counterterrorism Center
NDPC	National Domestic Preparedness Consortium
NGO	Nongovernmental Organization
NIAC	National Infrastructure Advisory Council
NIPP 2013	National Infrastructure Protection Plan 2013
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
OCI	Office of Criminal Investigations
OCIA	Office of Cyber and Infrastructure Analysis
OCIO	Office of the Chief Information Officer
OHA	Office of Health Affairs
OIE	World Organization for Animal Health
OIG	Office of the Inspector General
OMB	Office of Management and Budget
ORA	Office of Regulatory Affairs
OUP	Office of University Programs
PCII	Protected Critical Infrastructure Information
PPIA	Poultry Products Inspection Act
PPD	Presidential Policy Directive
R&D	Research and Development
RFR	Reportable Food Registry

RMA	Risk Mitigation Activity
S&T	Science and Technology Directorate
SAR	Sector Annual Report
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SFS	Secure Food Supply
SLTT	State, local, tribal, and territorial
SPPA	Strategic Partnership Program Agroterrorism
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
STHA	State and Territorial Health Agency
THIRA	Threat and Hazard Identification and Risk Assessment
USAID	United States Agency for International Development
U.S.C.	United States Code
USDA	United States Department of Agriculture
VS	Veterinary Services
WIFSS	Western Institute for Food Safety and Security
WMD	Weapons of Mass Destruction
ZADD	Zoonotic and Animal Disease Defense

A.1.2 Glossary of Terms

Agricultural and Food Product Storage. Establishments engaged in operating warehousing and storage facilities for agricultural and food products. These establishments provide facilities to store goods. They do not sell the goods they handle. These establishments take responsibility for storing the goods and keeping them secure. They may also provide a range of services, often referred to as logistics services, related to the distribution of goods.

Agriculture and Food. Agriculture comprises establishments primarily engaged in growing crops, raising animals, harvesting timber, and harvesting fish and other animals from a farm, ranch, or their natural habitats. Food establishments transform livestock and agricultural products into products for intermediate or final consumption. The industry groups are distinguished by the

raw materials (generally of animal or vegetable origin) processed into food and beverage products. The food and beverage products manufactured in these establishments are typically sold to wholesalers or retailers for distribution to consumers.

CARVER + Shock. An assessment methodology that provides a consistent means for evaluating the consequences, vulnerability, and threat faced by assets, systems, networks, and functions in the FA Sector. CARVER is an acronym for the six attributes used to evaluate the appeal of a target for attack: Criticality (measure of public health and economic impacts of an attack), Accessibility (ability to physically access and egress from target), Recuperability (ability of system to recover from an attack), Vulnerability (ease of accomplishing attack), Effect (amount of direct loss from an attack as measured by loss in production), and Recognizability (ease of identifying target). The seventh attribute, Shock, represents the combined health, economic, and psychological impacts of an attack.

Consequence Analysis. The estimate of the potential public health and economic impacts that a successful attack could cause.

Critical Infrastructure. The assets, systems, networks, and functions that provide vital services to the Nation.

Criticality. A description of the importance of a particular sector asset, system, network, or function in relation to national or regional security issues. Includes a consideration of public health and economic impacts.

Dependency. The one-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources to function properly.

Farm-to-Fork. Refers to the broad spectrum of industries responsible for all facets of food production, from where it is grown on the farm until it reaches the consumer's table.

FA Sector. The *National Strategy for Physical Protection of Critical Infrastructures and Key Assets* defines the sector as the supply chains for feed, animals, and animal products; crop production and the supply chains of seed, fertilizer, and other necessary related materials; and 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. In general terms, the sector is composed of the agricultural production and food systems from the farm to the table.

FA Sector Annual Report (SAR). A report prepared by the SSAs each year describing accomplishments in meeting SSP goals. The report includes details about specific programs

related to critical infrastructure protection, and SSAs submit the report to DHS for incorporation into the National Critical Infrastructure Annual Report.

Interdependency. Mutually reliant relationship between entities (objects, individuals, or groups). The degree of interdependency does not need to be equal in both directions.

Performance Measure. Indicator, statistic, or metric used to gauge program performance.

Processing/Packaging/Production. The transformation of livestock and agricultural products into products for intermediate or final consumption. This category is sometimes referred to as Food Manufacturing.

Regulatory, Oversight, and Industry Organizations. Organizations that provide technical, operation, pricing, and business oversight and support to the FA Sector.

Resilience. The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Risk. A measure of potential public health and economic harm that encompasses threat, vulnerability, and consequences.

Sector Partner. Federal and SLTT governments and private industry representatives from the FA Sector that partner together to enhance security for food and agricultural systems.

Secure and Security. Refer to reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.

Strategic Goal or Strategic Objective. A statement of aim or purpose included in a strategic plan (required under the Government Performance and Results Act of 1993). In a performance budget/performance plan, strategic goals group multiple program outcome goals. Each program outcome goal should relate to and in the aggregate be sufficient to influence the strategic goals or objectives and their performance measures.

Targets (performance). Refers to improved levels of performance needed to achieve the stated goals.

Threat Analysis. Estimates the likelihood that a particular target, or type of target, will be selected for attack, and is based on intent and capability of an adversary.

Appendix 2. USDA, FDA, SCC, and GCC Additional Information

As a result of PPD-21, DHS is responsible for coordinating the overall national effort to enhance security and resilience of all critical infrastructure of the United States. USDA and FDA have an obligation to provide leadership for sector infrastructure protection activities, including establishing information-sharing relationships and developing collaborative sector protection plans with sector partners. The FA Sector comprises a set of private industries (owners and operators), represented by the SCC, and government entities (Federal and SLTT), represented by the GCC.

HSPD-9 established a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies. USDA and FDA work together to submit an integrated budget plan for defense of the U.S. food system to the OMB Director. The investments of the Sector-Specific Agencies (SSAs) augment the Nation's food safety protection system and establish a partnership among the various organizations responsible for protecting the Nation's food supply. In addition, the SCC and GCC are responsible for encouraging vulnerability assessments.

A.2.1 USDA Key Authorities

USDA has a number of mission areas comprised of agencies and various departmental offices, each with extensive legal authorities.

Animal and Plant Health. APHIS is responsible for protecting and promoting U.S. agricultural health, administering the Animal Welfare Act, and carrying out wildlife damage management activities. The mission of APHIS is an integral part of USDA's efforts to provide the Nation with safe and affordable food. The Plant Protection Act, Animal Health Protection Act, Virus Serum Toxin Act, Agricultural Bioterrorism Protection Act of 2002, and the Animal Welfare Act are the primary statutory authorities used to achieve the agency's mission. These acts give APHIS the ability to restrict the importation, exportation, and interstate movement of plants, animals, plant and animal products, and plant and animal pathogens. They also provide APHIS with the authority to ensure that veterinary biologics are pure, safe, potent, and effective, and that the standards governing humane handling, care, and treatment of governed animals are met.

Domestic Nutrition Assistance. The Food and Nutrition Service (FNS) is the Federal agency responsible for managing USDA domestic nutrition assistance programs. Authorities for the administration of FNS nutrition assistance programs are in several places: the Child Nutrition Act of 1966 (42 U.S.C. 1786), as amended; the Richard B. Russell National School Lunch Act (42 U.S.C. 1751), as amended; the Food and Nutrition Act of 2008 (7 U.S.C. 2011), as amended; the

Agriculture and Consumer Protection Act of 1973, as amended; and the Emergency Food Assistance Act of 1983, as amended. Some food is purchased by USDA agencies for the nutrition assistance programs. Authorities to conduct purchase activities are provided for by five statutes: Section 32 of Public Law 74-320; the Richard B. Russell National School Lunch Act, as amended; the Agriculture and Consumer Act of 1973; the Emergency Food Assistance Act of 1983, as amended; and the Older Americans Act of 1964.

FNS is also responsible for disaster feeding in a presidentially declared disaster, using USDA commodity foods and Supplemental Nutrition Assistance Program (SNAP) benefits (if retail outlets are available). The statutory authority to purchase, use, and distribute food to victims of a presidentially declared disaster includes Section 412 and 413 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act); Section 5(h) of the Food and Nutrition Act of 2008, as amended; Section 416 of the Agricultural Act of 1949; Section 4(a) of the Agriculture and Consumer Protection Act of 1973; 7 CFR 280.1.

Food Processing (Meat, Poultry, and Egg Products). Food processors under USDA's jurisdiction are subject to the four key legal and statutory authorities under which FSIS operates. The Federal Inspection Acts that are most important to FSIS are the FMIA (21 U.S.C. 601 et seq.), the PPIA (21 U.S.C. 451 et seq.), and the EPIA (21 U.S.C. 1031 et seq.). Under the authority of these acts, FSIS provides continuous inspection of all meat, poultry, and egg products prepared for distribution in commerce, and re-inspects imported products to ensure that they meet U.S. food safety standards. FSIS tests for and conducts enforcement activities to address situations of microbiological, chemical, and other types of contamination, and conducts epidemiological investigations in cooperation with the CDC based on reports of foodborne health hazards and disease outbreaks. FSIS also carries out provisions of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Public Law 107-188). FSIS food defense initiatives are undertaken pursuant to the act. Additionally, the 1967 Wholesome Meat Act and the 1968 Wholesome Poultry Act direct FSIS to assess whether State inspection programs that regulate meat and poultry products are at least equal to the Federal program, in accordance with the 1967 Wholesome Meat Act and the 1968 Wholesome Poultry Act. Furthermore, the 1967 Wholesome Meat Act extended FSIS jurisdiction over meat and meat products, granting authority to regulate transporters, renderers, cold storage warehouses, and animal food manufacturers.

International Food Assistance. The U.S. Government has historically been involved with international food aid to help in disaster situations or where there is a need due to natural circumstances. Through various agencies, including Foreign Agricultural Service, international food aid is distributed to the needy in a variety of methods. Direct food aid, food aid through a distribution channel by way of private voluntary organizations or nongovernmental organizations, food aid to school children, and concessional loans are some of the methods by which a number of U.S. laws governing food aid are administered.

Through the Commodity Credit Corporation, USAID and USDA provide U.S. agricultural commodities to feed millions of hungry people in needy countries through direct donations and concessional programs. Food aid may be provided through four program authorities: (1) Public Law 480, also known as Food for Peace; (2) Food for Progress; (3) Section 416(b); and (4) the McGovern-Dole International Food for Education and Child Nutrition Program.

Marketing. The Agricultural Marketing Service (AMS) carries out a wide range of program activities that facilitate the marketing of U.S. agricultural production under the authorization of the Agricultural Marketing Act of 1946, the Perishable Agricultural Commodities Act, and more than 50 other statutes. These programs improve the efficiency of the national and international marketing of U.S. agricultural products by providing a language of trade and a network of marketing services that enhance returns to producers, lower prices to consumers, and help ensure fair trading in the marketplace. Two-thirds of the funds needed to finance AMS activities are derived from voluntary user fees charged for quality grading services. AMS provides these services to private industry, as well as Federal and State agencies.

A.2.2 FDA Key Authorities

FDA performs its public health duties pursuant to some of the following statutory authorities: Federal Import Milk Act (1927); Federal Food, Drug, and Cosmetic Act of 1938 (FFDCA), as amended; Public Health Service Act (1944); Fair Packaging and Labeling Act (1966); Infant Formula Act of 1980, as amended; Nutrition Labeling and Education Act of 1990; Dietary Supplement Health and Education Act of 1994; Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (the Bioterrorism Act); FDA FSMA (2011), and other related statutes. This list is not exhaustive, but illustrates the broad authority of FDA.

The FDA mission is mandated by the FFDCA and includes promoting and protecting human and animal health by ensuring that the nation's food supply is safe, sanitary, wholesome, and honestly labeled. The FFDCA defines food to include animal feed; however, for the purposes of this document, food refers to human food, and food for animals is referred to as feed. Under PPD-21, HHS, along with USDA, is assigned oversight of the FA sector. Other guidance and policy documents explaining FDA's authority and enforcement policies include Federal Register statements of policy and FDA Compliance Policy Guides.

Authorities from the FDA FSMA

FSMA (Pub. L. 111-353), signed into law by President Obama on January 4, 2011, enables FDA to better protect public health by helping to ensure the safety and security of the food supply. It enables FDA to focus more on preventing food safety problems rather than relying primarily on reacting to problems after they occur. The law also provides FDA with new enforcement authorities to help it achieve higher rates of compliance with prevention and risk-based food safety standards and to better respond to and contain problems when they do occur. The law also

gives FDA important new tools to better ensure the safety of imported foods and directs FDA to build an integrated national food safety system in partnership with State and local authorities.

For additional information on the regulations that are being developed in accordance with the FDA FSMA, please access http://www.fda.gov/fsma.

A.2.3 USDA/FSIS and HHS/FDA Jurisdictions Over Food

This table summarizes information concerning jurisdiction overlap for commercial products regulated by either or both FDA and USDA. It does not cover products made for onsite consumption such as pizza parlors, delicatessens, fast food sites, etc.

FDA JURISDICTION	USDA MEAT JURISDICTION	USDA POULTRY JURISDICTION	USDA EGG JURISDICTION
21 USC 392(b) Meats and meat food products shall be exempt from the provisions of this Act to the extent of the application or the extension thereto of the FMIA. FDA responsible for all non-specified red meats (bison, rabbits, game animals, zoo animals and all members of the deer family including elk (wapiti) and moose). FDA responsible for all non-specified birds including wild turkeys, wild ducks, and wild geese.	The FMIA regulates the inspection of the following amenable species: cattle, sheep, swine, goats, horses, mules or other equines, including their carcasses and parts. It also covers any additional species of livestock that the Secretary of Agriculture considers appropriate. Mandatory Inspection of Ratites and Squab (including emu) announced by FSIS April 2001.	The PPIA defines the term poultry as any domesticated bird. USDA has interpreted this to include domestic chickens, turkeys, ducks, geese, and guineas. The PPIA states poultry and poultry products shall be exempt from the provisions of the Federal Food, Drug, and Cosmetic Act to the extent they are covered by the PPIA. Mandatory Inspection of Ratites and Squab announced by FSIS April 2001.	The EPIA defines egg to mean the shell egg of domesticated chicken, turkey, duck, goose or guinea. Voluntary grading of shell eggs is done under USDA supervision. (FDA enforces labels/labeling of shell eggs.)
Products with 3% or less raw meat; less than 2% cooked meat or other portions of the carcass; or less than 30% fat, tallow or meat extract, alone or in combination. Products containing less than 2% cooked poultry meat; less than 10% cooked poultry skins, giblets, fat and poultry meat (limited to less than 2%) in any combination. *Closed-face sandwiches.	Products containing greater than 3% raw meat; 2% or more cooked meat or other portions of the carcass; or 30% or more fat, tallow or meat extract, alone or in combination.* Open-face sandwiches.	Products containing 2% or more cooked poultry; more than 10% cooked poultry skins, giblets, fat and poultry meat in any combination.*	Egg products processing plants (egg breaking and pasteurizing operations) are under USDA jurisdiction.

FDA JURISDICTION	USDA MEAT JURISDICTION	USDA POULTRY JURISDICTION	USDA EGG JURISDICTION
FDA is responsible for shell eggs and egg containing products that do not meet USDA's definition of "egg product." FDA also has jurisdiction in establishments not covered by USDA; e.g. restaurants, bakeries, cake mix plants, etc. Egg processing plants (egg washing, sorting, packing) are under FDA jurisdiction.			Products that meet USDA's definition of "egg product" are under USDA jurisdiction. The definition includes dried, frozen, or liquid eggs, with or without added ingredients, but mentions many exceptions. The following products, among others, are exempted as not being egg products: freeze-dried products, imitation egg products, egg substitutes, dietary foods, dried no-bake custard mixes, egg nog mixes, acidic dressings, noodles, milk and egg dip, cake mixes, French toast, sandwiches containing eggs or egg products, and balut and other similar ethnic delicacies. Products that do not fall under the definition, such as egg substitutes and cooked products, are under FDA jurisdiction.
Cheese pizza, onion and mushroom pizza, meat flavored spaghetti sauce (less than 3% red meat), meat flavored spaghetti sauce with mushrooms, (2% meat), pork and beans, sliced egg sandwich (closed-face), frozen fish dinner, rabbit stew, shrimp-flavored instant noodles, venison jerky, buffalo burgers, alligator nuggets, noodle soup chicken flavor.	Pepperoni pizza, meat-lovers stuffed crust pizza, meat sauces (3% red meat or more), spaghetti sauce with meat balls, open-faced roast beef sandwich, hot dogs, corn dogs, beef/vegetable pot pie.	Chicken sandwich (open face), chicken noodle soup.	

Jurisdiction for products produced under the School Lunch Program, for military use, etc., is determined via the same algorithm, although the purchases are made under strict specifications so that the burden of compliance falls on the contractor. Compliance Policy Guide 565.100, 567.200, and 567.300 provide additional examples of jurisdiction. IOM 3.2.1 and 2.7.1 provide more information on our interactions with USDA and Detention Authority.
* These percentages are based on the amount of meat or poultry product used in the product at formulation.

A.2.4 USDA and FDA Cybersecurity Infrastructure

The Federal Information Security Management Act (FISMA) requires that agencies have an effective information security program in place and delegate to the chief information officer (CIO) the authority to ensure compliance with requirements imposed on the agency under FISMA. The act further requires that the CIO designate a senior agency information security officer. The USDA CIO has delegated the associate chief information officer (ACIO) for Cyber Security to act as the USDA's senior agency information security officer.

The USDA Office of the Chief Information Officer's (OCIO) Cyber Security Program directs and administers the USDA Information Security Program in accordance with Federal regulations and

laws. In this capacity, the ACIO for cybersecurity directs the OCIO Cyber Security Program. In particular, the Cyber Security Program develops all cybersecurity policies in accordance with the NIST guidance. The ACIO for cybersecurity provides oversight of USDA agency and staff office information security programs and assistance to agency CIOs and information system security program managers; reviews and approves information system capital expenditures to ensure compliance with security policy and architecture; and develops risk management methodologies and tools to ensure compliance with related Federal Government and USDA regulations.

As part of the overall Cyber Security Program, OCIO uses several procedures, tools, and practices to continuously monitor the USDA Security Program:

- **Cyber Security Assessment and Management** is a comprehensive FISMA compliance tool developed by and for DOJ. It provides the ability to identify threats and vulnerabilities through the use of the embedded NIST Special Publication 800-53 (Rev. 1) control requirements for IT systems.
- **Program Reviews for Information Security Management Assistance** is a methodology for a standardized approach to review and measure the maturity of an information security program and outcomes of a review: identify information security program deficiencies; establish a security program baseline to measure future improvement following key personnel or organizational changes; validate completion of corrective actions or the "information security posture of the program"; provide supporting information for the FISMA scorecard and report; and prepare for or conduct an assessment, evaluation, or a review of an information security program.
- **FISMA Scorecard** is a centerpiece in monthly briefings to USDA's management. USDA maintained an aggressive posture toward IT security in several key areas.
- **Management Initiatives Tracking System Scorecard** is an interactive, Web-based database and management system that monitors and manages an agency's progress in implementing management initiatives. A new module was developed to integrate audit tracking processes. Data is tracked to monitor IT security and financial management weaknesses.

With the implementation HSPD-12, USDA led by example across the Federal Government in FY 2008. USDA made strides internally to prepare the infrastructure necessary to support the new HSPD-12 credential, the LincPass. USDA rolled out a comprehensive plan to implement two unique methods of verifying identity (two-factor authentication) processes and installed necessary hardware and software updates to enable 40 percent of targeted USDA laptops with the new security feature. USDA was at the forefront of deploying a nationwide mobile enrollment station project that took human and technological resources to USDA employees throughout the continental United States, Alaska, Hawaii, and Guam.

Every FDA cyber system has been assessed for potential risks and threats to define a mitigation action. In addition, CFSAN maintains an up-to-date security and contingency plan that details the steps to be taken if a system is compromised. Backup systems, alternative sites, and an overall center Continuity of Operations Plan support the system and the surrounding infrastructure.

A.2.5 Food and Agriculture Sector Coordinating Council (SCC) Governance Principles and Operating Procedures

Background, Mission and Purpose

FA sector company owners, operators, and trade associations have organized themselves in an alliance to proactively and dramatically foster advances in the way the industry, in partnership with State and Federal Government agencies, protects the Nation's food supply from farm-to-fork.

The SCC was created by the industry to serve the sector's counter-terrorism and security interests. SCC was formed using an inclusive and consultative process. The mission of the SCC is to:

- Facilitate intra-sector communications, set processes for information sharing, and facilitate priority setting regarding sector strategy and planning; policies and procedures; best management practices; threat communication and analysis; as well as sector protection, response and recovery planning and activities;
- Serve as the primary, policy-level interface with DHS and other Federal and State agencies on homeland security matters;
- Facilitate communications, plans, and activities with other relevant infrastructure sectors, government entities, and others necessary to further secure the nation's food supply and critical infrastructure; and
- Communicate the sector's needs and requests for resources to the government.

In considering new security structures, practices and procedures, the SCC will seek to combine new security practices with the already existing communication and food safety systems, as well as the science and technology already in place in the food and agriculture industry.

Composition

During the sector organizing process, it was agreed that the SCC will consist of representatives from subcouncils (currently seven). This process and structure are meant to result in the formation of one body (the SCC) that can accurately represent the scope, breadth, depth, and interdependence of the FA Sector (i.e., owners, operators, and their associations) on security

issues. Taken on their own, each of the initial seven subcouncils represents a significant component of the Nation's economy and critical food and agriculture infrastructure.

The SCC is made up of two designees and one alternate identified by each subcouncil. The three subcouncil representatives are expected to attend and participate in all SCC meetings. The two representatives and alternate from each subcouncil will be named by a consensus process by the subcouncil membership and will serve a two-year term on the SCC. Consecutive or non-consecutive subsequent terms are permitted.

- SCC members and alternates must, by definition, be employees of owners and operators of the sector or employees of their associations. Consultants, attorneys, or other representatives who are not employees or owners and operators of the sector or their associations cannot serve as SCC members or alternates.
- SCC alternates will automatically have decision-making authority when they sit in place of an absent member.
- In the event that a SCC member cannot, or chooses not to, fulfill the term of their office, the relevant subcouncil shall appoint a successor to fill the remainder of their term.

SCC Decision-Making, Roles, and Responsibilities

The SCC will make decisions using a consensus process rather than majority-rule voting. This is consistent with the approach the sector used to organize itself to ensure inclusion of the diverse segments of the FA Sector. Consensus is defined by a decision or action that all of the subcouncil represented on the SCC can live with (i.e., choose not to block). Each Subcouncil will have equal voice in decision-making processes and will be allowed one official position in consensus decision-making.

- Council members should collect and convey information effectively, efficiently, and inclusively to their subcouncil members; consult as broadly as possible on pending decisions and issues requiring feedback to the government or others outside the Council; and initiate liaison with others who can help serve the security needs of sector members and the interests represented by their subcouncil. This might include, but not be limited to, other critical infrastructure sectors, research and academic institutions, and others.
- Council members should play a leadership role in helping their subcouncil identify critical needs, problems, and opportunities for their own subcouncil area, as well as identify areas for linkage across subcouncil areas and to other critical infrastructure sectors or the government.

The responsibilities of SCC members are to:

- Represent and communicate the interests of their subcouncil to the Coordinating Council

and the government in sector matters;
- Keep subcouncil members appraised of key sector, inter-sector, and sector/government activities; and
- Bring to bear their best judgment upon SCC decisions based on their understanding and experience within their subcouncil business area.

SCC Meetings

- SCC meetings will be open to members and alternates as participants and to subcouncil members as observers. Leadership of each subcouncil will determine those subcouncil members that can attend SCC meetings as observers, which in large part will be driven by the issues to be discussed at the SCC meeting. Due to the potential size of SCC meeting audiences as a result of the open policy, subcouncil leaders will need to make notice of attendance early to the SCC Secretariat.
- SCC will meet on an as needed basis, as decided by the consensus of the council, but will initially meet in person with conference call-in capability at least once every three months in its first year of operation.
- SCC decisions can be made only when there is a quorum of participation (defined as at least one of the representatives or the alternate from each of the seven subcouncils). Because the SCC will make decisions by consensus, it will be possible (though not desirable) to conduct meetings with only one representative of any one subcouncil. The consensus decision-making process ensures that the protection of the interests of each subcouncil is respected. This process is based on a presumption that a subcouncil representative is in appropriate consultation and communication with her/his subcouncil. Therefore, each subcouncil must ensure that it has at least one of its three potential participants attending or participating in each session. In the event that none of the three representatives can attend, the subcouncil will select an individual to be granted decision-making authority for the subcouncil at that particular meeting. SCC members are expected to prepare for each meeting taking appropriate consultations with the subcouncil membership.

Principles of Participation in Council Meetings

- All members must be working towards the same goal and purpose of improving the nation's agriculture and food security system.
- All members need to participate by attending meetings, conference calls, and any other such activities whether called by the sector (industry) or the government.
- Discussion and deliberations must recognize and take advantage of each member's/organization's/subcouncil's strengths, skills, and perspective.

- Results of SCC discussion and deliberations must be a coherent voice made up of each member's and subcouncil's contributions.

SCC Secretariat

The Secretariat function for the SCC will be provided by DHS for CIPAC meetings only. Otherwise, SCC leadership maintains this function. The Secretariat will provide meeting and organizational support to include (but not limited to):

- Notifying members and alternates of meetings via email, telephone, or both;
- Distributing relevant background information prior to each meeting;
- Soliciting agenda topics for SCC and Joint Council Meetings based on communication with council members and alternates;
- Informing members and alternates of the agenda items, particularly decision items likely to be taken up at each council meeting on a timely basis;
- Arranging for meeting locations and support logistics;
- Taking and distributing meeting notes;
- Maintain and following up on a catalogue of SCC topic/issues and work products and their status;
- Ensuring ongoing liaison with the GCC and other external entities;
- Maintaining an updated mailing list for SCC members and alternates; and
- Identifying other support as needed and clarifying who should provide that support to the SCC.

Subject Matter Experts

Individual subject matter experts are non-voting participants of the SCC or any subcouncil drawn from any organization from which the SCC or a subcouncil needs expertise on an ad hoc basis. Subject matter experts may be invited to participate or assist the SCC or subcouncil by consensus agreement of the respective body.

Distribution of Material to the Sector

The SCC will identify or designate material requiring distribution and potential feedback such as reactions to existing or proposed government policies, plans, or activities. Specific guidance will accompany material such as purpose, timeline, nature of feedback desired, format, and means of communication if of a sensitive nature. Because the SCC is comprised of representatives of each subcouncil the SCC will heavily depend upon each subcouncil to establish clear procedures and

protocols for the distribution of information and material and the receipt of feedback, data, or other information.

Communication of Council Decisions and Meeting Summaries

The SCC will distribute a summary of its meetings and any decisions to the sector via the processes and procedures established by each subcouncil. Each subcouncil will convey procedures to the SCC and the Secretariat so that the means of distribution will be transparent to all within the sector. The SCC Secretariat will be responsible for 1) clarifying with the SCC membership that the meeting summaries and decisions are accurate prior to release for distribution and 2) distributing the final summaries and decision messages to each SCC member for communication to the subcouncil members as determined by each subcouncil' s standard procedures and practices.

Requested Meetings, Materials, and Briefings

While not required, briefings, meetings, and materials relevant to the interests of the FA Sector generally or which may involve interactive issues between subcouncils are encouraged to be conducted and conveyed to the SCC through the Secretariat. Briefings, meetings, and materials uniquely relevant to only one subcouncil and with no discernable interactive effects to other subcouncil areas in the sector should be conducted or conveyed at the subcouncil level. The default should be to err on the possibility of an integrative aspect and, hence, the primary area of action should be at the SCC level. When a subcouncil makes such a request they should notify the SCC Secretariat.

If the government seeks input of a general nature of interest to the FA Sector, it should make the request to the SCC via the Secretariat. As above, requests unique to a particular subcouncil should be made to that subcouncil if there are no discernable interactive or interdependencies to other subcouncils, but the SCC Secretariat should be notified and copied on the communications.

Sector Threat and Response

The SCC will provide a useful role in ensuring appropriate mechanisms for communicating confidential and sensitive information from the government to the industry via the subcouncils, and from the industry to the government on any actual, threatened, or suspected malicious attacks so the information may be analyzed.

Each subcouncil will be charged with the ability to create, interpret, and assess the proper response to a potential threat or attack as it relates to that subcouncil's specific area. Further, they

will develop the appropriate programs, procedures, and processes that will mitigate or reduce the vulnerabilities of their specific areas.

In the area of sector threats and response, the SCC and subcouncils will help in:

1. **Detecting potential threats to the food supply infrastructures.**
   - Working directly with DHS, USDA, and FDA and other government agencies, the SCC and subcouncils will be able to identify credible threats and craft specific warning messages to the food industry.
2. **Assessing threat information**.
   - Provide information and analysis information that will enable the food industry to report, identify, and reduce its vulnerability to malicious attacks.
3. **Providing timely warnings to the critical food supply operators so countermeasures can be developed and implemented.**
   - Facilitate the development of "best practices," recommendations, and countermeasures for preventing and recovering from malicious attacks.

SCC Subcouncils

Role, Responsibilities, and Principles of Participation

During the sector organizing process, sector members stressed the importance and essential nature of building sector coordination from clearly identified subcouncil areas called subcouncils.

- Each FA Sector subcouncil will develop definitions regarding the focus of the subcouncil to assist in identifying the focus and boundaries of its subcouncil areas, and so that members of the sector can clearly identify which subcouncil might involve their business and security interests.
- Each subcouncil will define its membership, priority issues, and areas of work and activity. Each subcouncil will need flexibility in prioritizing and identifying its needs, but should examine the general areas of communications and information sharing; R&D, including prevention and detection; incident management; vulnerability assessments; and recovery.
- Outreach, participation, and membership at the subcouncil level are intended to be as inclusive as possible of relevant owners and operators and their associations.
- Subcouncil will articulate their priorities and action items to the SCC, which then can communicate to the government, other sectors, and other appropriate entities

- Each subcouncil will determine its own procedures for naming representatives to the council (two from each with one alternate) as well as replacing a member or alternate. In addition, each subcouncil will take responsibility for naming an ad hoc SCC representative for any one meeting when none of its named individuals (i.e., the two members and one alternate) can attend. Subcouncils should give some consideration to identifying "high risk" food groups, which would be communicated to the SCC for consideration of additional inclusion in the SCC.
- Each subcouncil should establish its own decision-making procedures and operating procedures given the nature of the standard business practices and relationships in that part of the FA subcouncil.
- Each subcouncil might consider the use of subject matter experts, subcouncil member work groups, and/or advisory work groups to assist in their activities
- Each subcouncil should establish a procedure for soliciting subcouncil members' views on policies, programs, and activities, especially when conveying input to proposed or existing government policies, plans, procedures, and activities.
- Each subcouncil should establish and maintain subcouncil membership lists, contact information, and communication procedures for sensitive and non-sensitive information. These should be conveyed to the SCC and updated on a regular basis.

Other Elements of Sector Participation

Participation in subcouncils should be broad and inclusive. All those with a legitimate business interest and the ability to make a meaningful contribution should be encouraged to participate. Participation in multiple subcouncils is appropriate whenever legitimate business interests are served.

Subcouncil representation on the SCC is limited in order to maintain the efficiency of the SCC and consistency in subcouncil representation. In identifying members for the SCC, the following guidelines may be helpful.

1. Two SCC representatives plus one alternate are appropriate for each functioning subcouncil.
2. Representatives should be chosen from organizations whose business or whose members mirror the scope of the specific subcouncil as its members define it.
3. The individuals selected should be full-time employees of their organizations, minimizing the chances that any actual or perceived conflicts of interest may develop.

While an organization may participate in multiple subcouncils, an organization may represent only one of those subcouncils on the overall governing council.

A.2.6 Food and Agriculture Government Coordinating Council (GCC) Charter

Adopted December 4, 2014

Article I – Official Designation

This organization shall be known as the "FA Sector Government Coordinating Council," herein after referred to as the "GCC" or the "Council."

Article II – Mission and Purpose

PPD-21 advances national policy for Federal departments and agencies to identify and prioritize the United States' critical infrastructure, and to guard against efforts to undermine or exploit those sector assets. Federal departments and agencies will identify, prioritize and coordinate the protection of critical infrastructure. Federal departments will work with SLTT governments to develop a partnership with the private sector to leverage complementary resources within government, and between government and industry to ensure a more robust, resilient and secure sector. These identified critical infrastructures provide the essential services for American society; disruption could cause catastrophic health effects, mass casualties, negative impacts on economic well-being, or profoundly affect our national prestige and morale.

The designated SSAs for the FA Sector are USDA and HHS/FDA. In accordance with guidance provided by the Secretary of Homeland Security, these agencies shall collaborate with all relevant partners to prevent, deter and mitigate all-hazard risks to destroy, incapacitate or exploit the sector.

Article III – Objectives and Scope of Activity

Objective

The objective of the GCC is to support the Nation's homeland security mission by providing effective coordination of agricultural security and food defense strategies and activities; policy review and development; and communication across government and between the government and the private sector. In addition, the GCC plays a coordination role with the other SCCs.

The GCC acts as the counterpart and partner to the private industry-led SCC to plan and coordinate activities so that appropriate prevention, preparedness, response, and recovery systems are available to ensure that the Nation's food and agriculture critical infrastructure provides safe food and other agricultural products.

Scope of Activity

The GCC will accomplish this objective through the following essential activities:

- **Ensure efficient, effective policy coordination on homeland security issues.** The GCC shall bring together diverse Federal and SLTT interests to identify and develop collaborative strategies that advance critical infrastructure security and resilience. In addition, the GCC shall identify needs/gaps in security and resilience plans, programs, policies, procedures and strategies and leverage resources. Additionally, the GCC will ensure that strategies integrate roles, responsibilities, authorities and practices of GCC member organizations in support of coordinated preparedness and response to food and agriculture threats. The GCC leadership will also ensure coordination on these issues with the SCC.
- **Ensure efficient, effective communication concerning homeland security and emergency management issues.** While the focus is on IP, the GCC will also function during events of national emergency or significance to coordinate and share information to augment existing emergency operation channels within Federal and SLTT governments and with industry. The GCC leadership shall also ensure that effective communication mechanisms exist with the SCC.
- **Share information concerning successful programs and practices.** The GCC shall facilitate the sharing of experiences, ideas, best practices and innovative approaches related to critical infrastructure security and resilience. The GCC leadership shall coordinate with the SCC to ensure that both public and private successes are available for the sector.

Article IV – Membership and Member Representatives

Membership

The membership will be composed of key representatives and influential leaders on food and agriculture safety/defense issues from Federal and SLTT governments. Representatives to the GCC shall be active members of their respective governmental agency/academic entity and be nominated by their leadership via written notification to the GCC Co-Chairs. Official membership is conveyed once the GCC Co-Chairs acknowledge receipt of the nomination and submit the name of the member to DHS.

Member Representatives

Official members named to the Council are director-level, or equivalent, representatives from:

- U.S. Department of Agriculture*
- U.S. Department of Health and Human Services/FDA*
- U.S. Department of Homeland Security

- U.S. Department of Commerce
- U.S. Department of Defense
- U.S. Department of Interior
- U.S. Department of Justice
- U.S. Environmental Protection Agency
- Association of Food and Drug Officials
- Association of Public Health Laboratories
- American Association of Veterinary Laboratory Diagnosticians
- Association of State and Territorial Health Officials
- National Assembly of State Chief Livestock Health Officials
- National Association of State Departments of Agriculture
- National Association of County and City Health Officials
- National Environmental Health Association
- National Plant Board
- Intertribal Agriculture Council
- SLTT GCC
- DHS COEs
- Other SLTT government entities or academic institutions, as approved by the GCC Leadership

The SLTT Co-Chair is responsible for coordinating SLTT participation in FA Sector activities. The Co-Chair is expected to be a state or local government official/employee who has active responsibility for policy, operations, or program implementation in the FA Sector, thereby having experience and connections in the FA Sector and be willing to serve a 2 year term. This term may be amended by recommendations of the GCC Co-Chairs as circumstances warrant. In the event that the SLTT Co-Chair is no longer able to fulfill assigned responsibilities, a pre-designated alternate will serve in an acting capacity until the next Co-Chair is selected.

The GCC reserves the right to invite additional members as necessary to fulfill its mission.

Article V –Officers and Governance

Officers

The GCC leadership will be jointly chaired by the co-SSAs (USDA and FDA). In addition, the additional GCC Co-Chairs will be:

- Assistant Secretary, DHS/ IP (or their appointed representative)
- SLTT GCC Representative
    - Note: the SLTT GCC also nominates a Vice Chair who serves as an alternate to the SLTT GCC Co-Chair and is anticipated to fill the role of Co-Chair once the current Co-Chair completes their two year term. Both participate in GCC Leadership meetings.

Governance

The GCC leadership body will facilitate the decision-making process to improve preparedness of the sector using consensus-based methods. They will work in consultation with council membership to reach agreement on council business, and through this process, identify the steps by which each decision will be communicated to appropriate government or private sector entities. In the event consensus is not reached, GCC leadership will vote to reach an official decision.

Each member agency of the GCC may have one primary representative and one alternate representative for voting purposes. Both the primary and alternate may participate in all GCC meetings. Each member has the flexibility to have other representation at meetings other than the official alternates, but must clearly designate the representative's decision-making authority to the GCC Co-Chairs prior to the meeting.

The GCC may invite subject matter experts, non-voting participants drawn from any organization, to provide expertise on an ad hoc basis.

Recognizing the criticality of providing effective communication across the government and private sectors, members shall act as Sector communication liaisons for their respective agencies and organizations. As such, they shall accept the responsibility of passing information between the GCC and their respective agency and organization constituents. This established information flow is critical to support national communications and provide a national alert capability for the FA Sector and its diverse stakeholders. The membership will support and execute this responsibility.

Article VI – Meetings

The GCC will meet on a monthly basis, primarily through conference calls, with additionally scheduled meetings and/or conference calls as needed. The GCC reserves the right to amend the frequency of the meeting and location to meet its mission.

Principles of Participation

- All members must be working towards the same goal and purpose of improving the Nation's agriculture and food system security.
- All members need to participate.
- Discussions and deliberations must recognize and take advantage of each member/organization's strengths, skills and perspective.
- Results of GCC discussions and deliberations must be a coherent voice comprised of each member's contributions.
- Each discussion shall be honest and forthright.

Meeting Governance

Discussion and deliberations must recognize and take advantage of each member's and organization's strengths, skills, and perspective.

1. The lead will canvass GCC members prior to the scheduled meeting for priorities and agenda topics.

2. The GCC will hold its discussion for a set amount of time or upon agreement/closure, bringing in subject matter experts as needed.

3. The lead member will ask for GCC agreement for continuation/completion/reconsideration for each agenda topic.

4. If substantial work effort is required through work groups, the lead member will appoint a GCC member to lead the work group.

Decision-Making

Council members will make decisions through a consultative process, encouraging the exchange of information and points of view, and will strive for consensus. Although any member may disagree with a decision, other members will strive to understand and resolve disagreements. Dissension will be recognized and reasons clearly understood by all other members when a member absolutely cannot agree. When there is dissension, the Council may move forward and take action, nevertheless to fulfill obligations of members of the Council. GCC leaders/members will strive to meet timeliness and deliverables even when less than full agreement is reached.

The Council recognizes that each member represents a government entity or organization with inherent legal authorities and parameters within which they must operate. At times, these authorities may restrict a member's ability to provide agreement on a decision. These inherent legal authorities must be clearly articulated and understood by the Council as the basis for dissent and the inability to enter into consensus.

Quorum

In the event that a decision needs to be made by vote, a quorum for decision-making is defined as consisting of at least one representative from each of the co-SSAs (USDA and FDA), DHS, an SLTT member, and three (3) other GCC member organizations.

Article VII – Recordkeeping

Recordkeeping responsibilities, to include the development of meeting notes, reside with the SSA Co-Chairs. Meeting summaries are available upon request by members. Critical Infrastructure Partnership Advisory Council (CIPAC) meeting records shall also be maintained by the DHS Secretariat.

Article VIII – Communications

A current e-mail distribution list of Council members will be maintained and dedicated for official Sector activity use only. Only the Co-Chairs may use this list.

The GCC is a coordination council that guides policy across Government agencies. Decisions and information discussed and shared in GCC meetings should not be distributed outside of the GCC, as it may have policy implications. GCC information should not be divulged until it has been formally released.

Article IX – Working Groups and Special Committees

Establishing Work Groups

The Council may establish work groups to conduct substantial investigation, research, and/or development, which cannot be achieved by a regular session of the Council. The GCC must provide the group a specific and clear charge, time limit, and deliverable as part of initiating the work group. The group's representation will be determined by the scope of the topic. Each group will include a GCC member to lead the activity and maintain continuity and consistency.

Article X – CIPAC Membership and Representation

Council Participation in CIPAC

As explained in the CIPAC Charter, the Secretary of Homeland Security established the CIPAC in March 2006, and exempted the CIPAC from the Federal Advisory Committee Act.

CIPAC facilitates interaction between government officials and representatives of the community of owners and/or operators for each of the 16 critical infrastructure sectors defined by PPD-21 and identified in NIPP 2013. When participating in CIPAC activities, the Council will comply with all requirements defined in the CIPAC Charter and guidance issued by the CIPAC Designated Federal Officer (DFO) within the CIPAC Executive Secretariat.

The GCC, in coordination with the SCC, participates in CIPAC activities as appropriate. For example:

- Joint GCC/SCC Meetings
- GCC and SCC Leadership Meetings

CIPAC Member and CIPAC Member Representative

CIPAC membership is defined in the CIPAC Charter. GCC membership shall be in compliance with CIPAC Charter requirements. GCC member organizations shall automatically be a CIPAC Member upon notification from the Council Chairperson to the CIPAC DFO via CIPAC@hq.dhs.gov.

A CIPAC Member may have more than one CIPAC Member Representative. The Member Representative's name and contact information shall be added to the CIPAC Attendee Roster upon notification to the CIPAC DFO by the Council Chairperson via CIPAC@hq.dhs.gov.

The procedures for maintaining a CIPAC Member Representative list within the Council are as follows:

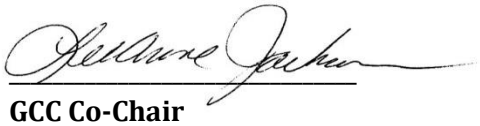
- To appoint duly authorized member representatives to participate in CIPAC activities, organizations shall provide the GCC Co-Chairs with the representative's name and contact information in written form. The Co-Chairs shall provide this information to DHS Secretariat for transmission to DFO on behalf of the Sector leadership.
- The DHS Secretariat, in collaboration with the Co-Chairs, shall maintain a current GCC member roster and periodically update the CIPAC DFO with member information in order to maintain a compliant CIPAC Attendee Roster.

Article XI – Amendments

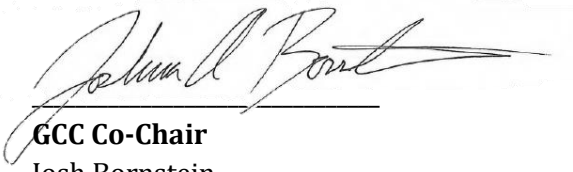
Amendments to the GCC Charter may be authorized with two-thirds of member consent and the presence of quorum.

Article XII – Approval

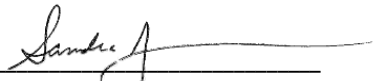
This Charter will be approved with two-thirds of member consent and the presence of quorum.



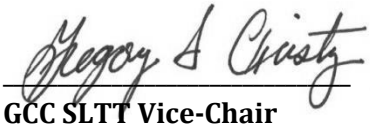
GCC Co-Chair
LeeAnne Jackson
Health Science Policy Advisor
U.S. Department of Health and Human Services
Food and Drug Administration
Center for Food Safety and Applied Nutrition



GCC Co-Chair
Josh Bornstein
Senior Policy Advisor
U.S. Department of Agriculture
Office of Homeland Security and Emergency Coordination
National Security Policy Staff



GCC SLTT Chair
Sandy Johnson
Emergency Management Coordinator
State of Kansas
Department of Agriculture



GCC SLTT Vice-Chair
Greg Christy
Veterinary Manager
State of Florida
Department of Agriculture and Consumer Services

Appendix 3. Academia and Research Centers

A.3.1 National Center for Zoonotic and Animal Disease Defense

Founded in April 2004 as a DHS COE, ZADD conducts research and develops prototypes to protect the United States from foreign, emerging and zoonotic, or high consequence animal diseases that threaten public health and economic stability. The ZADD COE is composed of a consortia of academic and private sector partners co-led by IIAD at Texas A&M University founded in 2004 and the COE in Emerging and Zoonotic Animal Diseases (CEEZAD) at Kansas State University founded in 2010.

The ZADD COE focuses on zoonotic diseases that pose catastrophic risks to human health, livestock health, and the national agricultural economy. Zoonotic diseases infect both humans and animals and are transmissible between them. At least 60 percent of all human pathogens are zoonotic, according to the CDC. Seventy-five percent of emerging, infectious human diseases began as infectious animal diseases.

The IIAD mission is to create products that will protect against the introduction of high-consequence diseases to the United States, with an emphasis on prevention, surveillance, intervention, and recovery.

IIAD products and projects are organized by the Institute's thematic categories, including:

- **Biological Systems.** Vaccines, anti-viral agents, detection and diagnostic tests and universal platforms that satisfy DHS goals of detection, diagnosis, prevention and recovery;
- **Information and Analysis Systems.** Modeling and analysis tools to support better informed decision-making at multiple levels of scale; and
- **Education and Outreach.** Graduate programs, early responder training, and stakeholder workshops to provide the next generation of science power for homeland security.

The CEEZAD mission is to enhance the capability of DHS by developing "state of the art" countermeasures for high priority emerging and zoonotic animal diseases.

CEEZAD products and projects are organized by research themes, including:

- **Vaccines.** Novel vaccine candidates against known and newly emerging threat agents, new vaccine platforms for rapid development.
- **Detection.** Serologic assays capable of differentiating between infected and vaccinated animals in support of vaccine studies, rapid multiplex PCR assays for differential detection,

novel diagnostic platforms for rapid detection of unknown agents.

- **Epidemiology and Modeling.** Zoonotic and emerging animal disease transmission and economic modeling.
- **Education and Outreach.** Support students through Master of Public Heath (MPH), Doctor of Veterinary Medicine (DVM), and Doctor of Philosophy (PhD) programs to prepare for high consequence disease events and interact with the HSE.

A.3.2 National Center for Biomedical Research and Training

The National Center for Biomedical Research and Training (NCBRT), which began at Louisiana State University in 1998, provides training to emergency responders throughout the United States. NCBRT is part of the National Center for Security Research and Training, as well as the National Domestic Preparedness Consortium (NDPC), recognized by DHS as the principal vehicle through which the Training and Exercise Integration Division identifies, develops, tests, and delivers training to Federal, State, local, and tribal emergency responders. The NCBRT mission is to help America prevent, prepare for, respond to, and recover from acts of domestic and international terrorism, WMD, and high-consequence events through teaching, training, technical assistance, and research. NCBRT strives to be a pace-setting organization that is committed to preparing America today for tomorrow's threats.

NCRBT is involved on a national scale in research, curricula development, training, and other projects in the areas of WMD, mass casualty incidents, and counterterrorism. As a founding member of NDPC, NCBRT is one of seven partners that identifies, develops, tests, and delivers training to State and local emergency responders. NCBRT goals include:

- Prepare America to address its threats;
- Expand the NCBRT business and financial bases to ensure fiscal viability and continuity;
- Recruit and retain highly qualified people who will accept the mission, embrace the vision, and embody the core values; and
- Expand and strengthen the NCBRT relationships among colleagues, customers, and competitors.

A.3.3 Food Protection and Defense Institute

FPDI (previously called the National Center for Food Protection and Defense) was officially launched as a DHS COE in July 2004. FPDI addresses the vulnerability of the Nation's food system to attack through intentional contamination with biological or chemical agents.

The FPDI research and education program is aimed at reducing the potential for contamination at any point along the food supply chain and mitigating potentially catastrophic public health and

economic effects of such attacks. The program incorporates cutting-edge research across a wide range of disciplines, taking a comprehensive, farm-to-fork view of the food system and encompassing all aspects from primary production through transportation and food processing to retail and food service.

In delivering on its mission to defend the safety and security of the food system through research and education, FPDI places a high priority on addressing potential threats to the food system that could lead to catastrophic damage to public health or the economy.

Specific program goals include:

- Significant improvement in supply chain security, preparedness, and resiliency;
- Development of rapid and accurate methods to detect incidents of contamination and to identify specific agents involved;
- Application of strategies to reduce the risk of foodborne illness resulting from intentional contamination in the food supply chain;
- Development of tools to facilitate recovery from contamination incidents and resumption of safe food system operations;
- Rapid mobilization and delivery of appropriate and credible risk communication messages to the public; and
- Delivery of high-quality education and training programs to develop a cadre of professionals equipped to deal with future threats to the food system.

More than 150 experts from academia, private sector research organizations, professional organizations, State and Federal Government agencies, and the food industry are currently involved in the FPDI research and education program. FPDI research teams are organized thematically in systems (supply chain, public health response, and economic analysis), agents (detection, inactivation, and decontamination), and training (risk communication and education).

Academic collaborators are University of Minnesota, Michigan State University, University of Wisconsin at Madison, North Dakota State University, Georgia Institute of Technology, University of Tennessee at Knoxville, and individual investigators from 21 other universities.

A.3.4 The Extension Disaster Education Network

The Extension Disaster Education Network (EDEN) is a collaborative multistate effort by Extension services across the United States, enabling them to use and share resources to improve the delivery of services to citizens affected by disasters. The EDEN mission is to reduce the impact of disasters through research-based education, including:

- Interdisciplinary and multi-State research and education programs addressing disaster

mitigation, preparation, response, and recovery;
- Linkages with Federal, State, and local agencies and organizations;
- Timely and prompt communications and delivery of information that meets audience needs;
- Anticipation of future disaster education needs and actions; and
- Credible and reliable information.

EDEN delegates communicate informally through an e-group maintained by Michigan State University. The delegates meet annually, usually in the fall. The EDEN Web site receives support from the CSREES.

A.3.5 International Food Protection Training Institute

In March 2009, the Association of Food and Drug Officials was awarded a $2 million grant from the W.K. Kellogg Foundation to create and develop the International Food Protection Training Institute (IFPTI). While the overall purpose of the training institute is to address the unmet educational needs of food protection professionals, its immediate focus will be on the urgent need for standardized, graduated, and career-spanning training of State and local food protection professionals to meet generally recognized food safety standards.

IFPTI will fill in gaps in the development or delivery of training essential for food protection by improving and maintaining the knowledge and skills of people who work in the food safety community. The IFPTI will record and provide, but not duplicate, training developed or delivered to food protection professionals by others.

The certified curricula will meet specific standards, span a professional's entire career, and serve as an umbrella to incorporate existing training programs. IFPTI delivered its inaugural training course, "Managing Retail Food Safety," on July 14–16, 2009.

A.3.6 Additional Research Centers

Iowa State University

The Center for Food Security and Public Health at Iowa State University works to increase awareness of bioterrorism, agroterrorism, FADs, and zoonotic diseases; provide tools on biological risk management; and assist State and local governments to prepare for animal emergencies.

Kansas State University

The National Agricultural Biosecurity Center was established by Kansas State University to coordinate interdisciplinary activities focused on protecting U.S. agricultural infrastructure and

economy from endemic and emerging biological threats. In addition, Kansas State formed the Food Science Institute in 2001 to facilitate initiatives across 5 colleges and 11 departments. Food Safety and Security is one of the major program areas of the Food Science Institute.

Pennsylvania State University

Food Safety Programs in the Penn State Department of Food Science enhance food safety by providing a collaborative and multidisciplinary approach that integrates research, teaching, and outreach.

Purdue University

The National Biosecurity Resource Center at Purdue University is dedicated to providing educational and resource opportunities for the protection and sustainment of the health and wellbeing of companion animals, livestock, and food supply.

South Dakota State University

"Food Defense: Security in a Foodservice Operation" is a DVD developed by the South Dakota State University Cooperative Extension Service in cooperation with FSIS. While the title implies it is for foodservice businesses, the information contained in the DVD can apply to any business. The video covers assessing risks to a business, developing contingency plans, communicating plans with employees, and implementing plans.

University of California, Davis

The Western Institute for Food Safety and Security (WIFSS) at the University of California, Davis is a training partner of the FEMA Protection and National Preparedness Directorate at DHS and is tasked with the development and delivery of DHS certified agroterrorism courses. The overall goal of WIFSS is to enhance national security by strengthening preparedness of the frontline responders to ensure capacity to respond early, effectively, and in coordination with State and Federal agencies.

University of Georgia

The Center for Food Safety at the University of Georgia partners with food industry to engage in research for the maintenance and improvement of the microbiological safety of the world's food supply. In addition, it is the only institution in the United States offering an Agrosecurity Certificate Program, which attracts and motivates students to think critically about emerging issues in food system infrastructure, policy, and security.

University of Maryland

Jointly administered by the University of Maryland and FDA, the Joint Institute for Food Safety and Applied Nutrition (JIFSAN) is the foundation of public and private partnerships. JIFSAN provides the scientific basis for ensuring a safe and wholesome food supply and the infrastructure for contributions to national food safety programs and international food standards.

University of Minnesota

The Center for Infectious Disease Research and Policy at the University of Minnesota is a global leader in addressing public health preparedness and emerging infectious disease response.

University of New Mexico

The Sustainability Studies Program at the University of New Mexico has begun a coordinated effort to develop a carbon-neutral food shed for the State of New Mexico. The Program mission statement is to create a thriving New Mexico food supply system while contributing to a balanced carbon budget.

University of Tennessee

The Food Safety COE at the University of Tennessee develops and evaluates strategies to destroy or control foodborne pathogens and reduce the occurrence of foodborne illnesses. Also at the University in the College of Veterinary Medicine, the Center for Agriculture and Food Security and Preparedness is dedicated to helping protect agriculture and food supply critical infrastructure across the Nation.

Appendix 4. FA Sector RMAs

The following list, while not intended to prioritize in a formal manner, is an attempt to illustrate the FA Sector's ongoing and proposed RMAs:

a) Laboratory networks;

b) Information-sharing protocols and procedures;

c) FA response and recovery exercises;

d) Countermeasures for emergency response to a food contamination or animal health event;

e) Pre-harvest risk assessments;

f) Post-harvest (food) risk assessments;

g) Planning and preparedness assistance for owners and operators;

h) FA defense training and awareness materials development and distribution;

i) Pre-harvest surveillance programs for animal and plant pathogens;

j) Post-harvest (food) R&D for biological, chemical, and radiological agents;

k) Pre-harvest R&D efforts;

l) Post-harvest (food) surveillance for biological and chemical agents;

m) Programs for recovery assistance development; and

n) NIST Cybersecurity Framework Implementation guidance.

Appendix 5. FA Sector Crosswalk Tables

Table A.5-1: Contribution of FA Sector Priorities to JNP and NIPP Goals

NIPP Goals	JNP Strengthen the Management of Cyber and Physical Risks to Critical Infrastructure	JNP Build Capabilities and Coordination for Enhanced Incident Response and Recovery	JNP Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines	JNP Enhance Effectiveness in Resilience Decision Making	JNP Share Information to Improve Prevention, Mitigation, Response, and Recovery Activities
Assess and analyze risks to critical infrastructure (Threat, Vulnerability, Consequence) to inform risk management activities.	FA Priority #3	FA Priority #1, 3		FA Priority #1	FA Priority #3
Secure critical infrastructure against physical, cyber, and human threats through sustainable risk reduction efforts, while considering costs and benefits.	FA Priority #3	FA Priority #1, 3		FA Priority #1	FA Priority #3
Enhance critical infrastructure resilience by minimizing consequences and employing effective response and recovery.	FA Priority #3	FA Priority #1, 3, 4		FA Priority #1	FA Priority #3

NIPP Goals	JNP Strengthen the Management of Cyber and Physical Risks to Critical Infrastructure	JNP Build Capabilities and Coordination for Enhanced Incident Response and Recovery	JNP Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines	JNP Enhance Effectiveness in Resilience Decision Making	JNP Share Information to Improve Prevention, Mitigation, Response, and Recovery Activities
Share information across the critical infrastructure community to build awareness and enable risk-informed decision-making.	FA Priority #3	FA Priority #3	FA Priority #2, 5		FA Priority #2, 3, 5
Promote learning and adaptation during and after incidents and exercises.			FA Priority #5		FA Priority #5

Table A.5-2: Contribution of FA Sector Priorities to NIPP Calls to Action

Call to Action Activities	FA Sector Priority 1	FA Sector Priority 2	FA Sector Priority 3	FA Sector Priority 4	FA Sector Priority 5
1. Set national focus through jointly developed priorities.					
2. Determine collective actions through joint planning efforts.			✓		
3. Empower local and regional partnerships to build capacity nationally.	✓				✓
4. Leverage incentives to advance security and resilience.	✓		✓		✓
5. Enable risk-informed decision-making through		✓			✓

Call to Action Activities	FA Sector Priority 1	FA Sector Priority 2	FA Sector Priority 3	FA Sector Priority 4	FA Sector Priority 5
enhanced situational awareness.					
6. Analyze infrastructure dependencies, interdependencies, and associated cascading effects.			✓		✓
7. Identify, assess, and respond to unanticipated infrastructure cascading effects during and following incidents.	✓				
8. Promote infrastructure, community, and regional recovery following incidents.			✓	✓	✓
9. Strengthen coordinated development and delivery of technical assistance, training, and education.					
10. Improve critical infrastructure security and resilience by advancing R&D solutions.	✓				
11. Evaluate progress toward the achievement of goals.					
12. Learn and adapt during and after exercises and incidents.					✓

Table A.5-3: Alignment of NIPP Goals with Calls to Action, JNP, and Cybersecurity Framework

Call to Action Activities	NIPP Goals Assess and Analyze Risks to Critical Infrastructure to Inform Risk Mgmt. Activities	NIPP Goals Secure Critical Infrastructure Against Threats While Considering Costs and Benefits	NIPP Goals Enhance Critical Infrastructure Resilience by Minimizing Consequences & Employing Effective Response and Recovery	NIPP Goals Share Information to Enable Risk Informed Decisions	NIPP Goals Promote Learning & Adaptation During/After Incidents and Exercises
1. Set national focus through jointly developed priorities.	✓	✓	✓	✓	✓
2. Determine collective actions through joint planning efforts.	✓	✓	✓	✓	✓
3. Empower local and regional partnerships to build capacity nationally.			✓		
4. Leverage incentives to advance security and resilience.		✓	✓		
5. Enable risk-informed decision-making through enhanced situational awareness.				✓	
6. Analyze infrastructure dependencies, interdependencies, and associated cascading effects.	✓		✓		

Call to Action Activities	NIPP Goals Assess and Analyze Risks to Critical Infrastructure to Inform Risk Mgmt. Activities	NIPP Goals Secure Critical Infrastructure Against Threats While Considering Costs and Benefits	NIPP Goals Enhance Critical Infrastructure Resilience by Minimizing Consequences & Employing Effective Response and Recovery	NIPP Goals Share Information to Enable Risk Informed Decisions	NIPP Goals Promote Learning & Adaptation During/After Incidents and Exercises
7. Identify, assess, and respond to unanticipated infrastructure cascading effects during and following incidents.			✓		
8. Promote infrastructure, community, and regional recovery following incidents.			✓		
9. Strengthen coordinated development and delivery of technical assistance, training, and education.					✓
10. Improve critical infrastructure security and resilience by advancing R&D solutions.		✓	✓		
11. Evaluate progress toward the achievement of goals.					✓
12. Learn and adapt during and after exercises and incidents.					✓

Draft JNP Activities	NIPP Goals Assess and Analyze Risks to Critical Infrastructure to Inform Risk Mgmt. Activities	NIPP Goals Secure Critical Infrastructure Against Threats While Considering Costs and Benefits	NIPP Goals Enhance Critical Infrastructure Resilience by Minimizing Consequences & Employing Effective Response and Recovery	NIPP Goals Share Information to Enable Risk Informed Decisions	NIPP Goals Promote Learning & Adaptation During/After Incidents and Exercises
Strengthen the management of cyber and physical risks to critical infrastructure.	✓	✓	✓	✓	
Enhance effectiveness in resilience decision-making.	✓	✓	✓	✓	
Strengthen collaboration across sectors, jurisdictions, and disciplines.			✓	✓	✓
Build capabilities and coordination for enhanced incident response and recovery.			✓	✓	✓
Share information to improve prevention, mitigation, response, and recovery activities.	✓	✓	✓	✓	✓

Cybersecurity Framework Performance Goals	NIPP Goals Assess and Analyze Risks to Critical Infrastructure to Inform Risk Mgmt. Activities	NIPP Goals Secure Critical Infrastructure Against Threats While Considering Costs and Benefits	NIPP Goals Enhance Critical Infrastructure Resilience by Minimizing Consequences & Employing Effective Response and Recovery	NIPP Goals Share Information to Enable Risk Informed Decisions	NIPP Goals Promote Learning & Adaptation During/After Incidents and Exercises
Critical systems and functions are identified and prioritized, and cyber risk is understood as part of a risk management plan.	✓				
Risk-informed actions are taken to protect critical systems and functions.		✓			
Resources are coordinated and applied to triage and respond to cyber events and incidents in order to minimize impacts to critical systems and functions.			✓		
Following a cyber incident, impacted critical systems and functions are reconstituted based on prior planning and informed by situational awareness.			✓		
Adverse cyber activities are detected and situational awareness of threats is maintained.				✓	

Cybersecurity Framework Performance Goals	NIPP Goals Assess and Analyze Risks to Critical Infrastructure to Inform Risk Mgmt. Activities	NIPP Goals Secure Critical Infrastructure Against Threats While Considering Costs and Benefits	NIPP Goals Enhance Critical Infrastructure Resilience by Minimizing Consequences & Employing Effective Response and Recovery	NIPP Goals Share Information to Enable Risk Informed Decisions	NIPP Goals Promote Learning & Adaptation During/After Incidents and Exercises
Security and resilience are continually improved based on lessons learned, consistent with risk management planning.					✓

Appendix 6. DHS Infrastructure Data Taxonomy for the FA Sector

Critical infrastructure and their elements can be described and categorized in various ways, which can result in inconsistent communication and hinder timely decision-making in the homeland security community. To prevent such problems, DHS uses an Infrastructure Data Taxonomy to enable transparent and consistent communication about critical infrastructure between government and private sector partners.

The following terms describe the information in the FA Sector Infrastructure Data Taxonomy:

- **Taxonomy Identification Code.** This is an internal code and does not refer to any sector-specific code that may be in use.
- **North American Industry Classification System (NAICS) Code.** The taxonomy is based broadly on the NAICS code. The code number that most closely corresponds to the asset is provided. NAICS was developed jointly by the United States, Canada, and Mexico to allow comparison of business statistics. Although not developed specifically for use with infrastructure, the NAICS code can be used to help define the type or purpose of a facility and annotate the infrastructure categorization. Because some assets do not fit into the NAICS code structure, an approximate NAICS code is assigned where possible. (Significant approximations are identified in parentheses.) While NAICS is a worthy guide, SSAs are the primary driver of the taxonomy layout and definition. In this version of the taxonomy, each sector was given the opportunity to provide input, when possible, to be incorporated into the taxonomy regardless of the NAICS code. In this version of the taxonomy, some sectors have been completely changed from previous versions. Thus, they may not have a NAICS-assigned or NAICS-related code.
- **Description.** A summary of the types of assets that fall into each category. To the extent possible, these descriptions were developed from standard definitions used by each industry. SSAs had an opportunity to provide input, and the definitions were compiled to follow that input, to the extent possible.
- **Attributes of Interest.** Key attributes of an asset that help better define the facility. Attributes could include size, type of equipment, operational capacity, volume of production, or a wide range of other attributes. Only a few of the most significant attributes are included.
- **Other Categorization.** In some cases, an asset could be included in more than one sector. Inclusion in more than one sector helps define possible interdependencies or additional categorizations for use in various models and database tools. For example, a dam with a hydroelectric power plant can be categorized in the Dams Sector, but it can also be cross-

referenced in the Energy Sector because the hydroelectric power plant is located at the dam.

Table A.6-1 shows the FA Sector Taxonomy provided by DHS. To download or comment on the Taxonomy, please visit: http://www.dhs.gov/infrastructure-data-taxonomy.

Table A.6-1: FA Sector Infrastructure Taxonomy

ID	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1		**AGRICULTURE AND FOOD** Agriculture comprises establishments primarily engaged in growing crops, raising animals, harvesting timber, and harvesting fish and other animals from a farm, ranch, or their natural habitats. Food establishments transform livestock and agricultural products into products for intermediate or final consumption. The industry groups are distinguished by the raw materials (generally of animal or vegetable origin) processed into food and beverage products. The food and beverage products manufactured in these establishments are typically sold to wholesalers or retailers for distribution to consumers.		
1.1		**SUPPLY** Facilities that supply the livestock and agricultural raw materials.		
1.1.1	111	**Crop Production** These facilities comprise establishments, such as farms, orchards, groves, greenhouses, and nurseries, primarily engaged in growing crops, plants, vines, or trees and their seeds.		
1.1.1.1	1111	*Oilseed and Grain Farms* Farms are engaged in growing oilseed and/or grain crops and/or producing oilseed and grain seeds. These crops have an annual life cycle and are typically grown in open fields. Includes soybeans, oilseeds, dry pea and beans, wheat, corn, oats, rice, and others.	• Acreage • Crop(s) Produced • Production	
1.1.1.2	1112	*Vegetable and Melon Farms* *Farms primarily engaged in growing root and tuber crops(except sugar beets and peanuts) or edible plants and/or producing root and tuber or edible plant seeds. The crops included in this group have an annual growth cycle and are grown in open fields. Climate and cultural practices limit producing areas, but often permit the growing of a combination of crops in a year.*	• Acreage • Crop(s) Produced • Production	

ID Code	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1.1.1.3	1113	*Fruit and Tree Nut Farms* These farms are primarily engaged in growing fruit and/or tree nut crops. The crops included are generally not grown from seeds and have a perennial life cycle. Includes citrus and non-citrus fruits and nuts.	• Acreage • Crop(s) Produced • Production	
1.1.1.4	1114	*Greenhouse, Nursery, and Floriculture Facilities* Facilities primarily engaged in growing crops of any kind under cover and/or growing nursery stock and flowers. "Under cover" is generally defined as greenhouses, cold frames, cloth houses, and lath houses. The crops grown are removed at various stages of maturity and have annual and perennial life cycles. The nursery stock includes short rotation woody crops that have growth cycles of ten years or less.	• Crop(s) Produced • Facility Area • Production	
1.1.1.5	1119	*Other Crop Farms* These farms grow crops, such as tobacco, cotton, sugarcane, hay, sugar beets, peanuts, agave, herbs and spices, and hay and grass seeds or grow a combination of crops (except a combination of oilseed(s) and grain(s) and a combination of fruit(s) and tree nut(s)).	• Acreage • Crop(s) Produced • Production	
1.1.2	112	**Animal Production** Facilities in this category raise or fatten animals for the sale of animals or animal products, and are comprised of ranches, farms, and feedlots primarily engaged in keeping, grazing, breeding, or feeding animals. The animals are generally raised in various environments, from total confinement or captivity to feeding on an open range pasture.		
1.1.2.1	1121	*Cattle Ranches and Farms* Facilities primarily engaged in raising cattle, milking dairy cattle, or feeding cattle for fattening.		
1.1.2.1.1	112111	*Beef Cattle Ranches* Establishments primarily engaged in raising cattle (including cattle for dairy herd replacements)	• Head of Cattle Production	

ID Code	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1.1.2.1.2	11211	*Livestock Order Buyers* Livestock dealers who purchase or hold livestock (generally for up to one week) while the animals are aggregated into a large enough group to meet specific customer orders.	• Head of Cattle Handled	
1.1.2.1.3	11211	*Livestock Backgrounders* Establishments that condition livestock between pasture and feedlots (generally for up to several weeks) so they will grow well in feedlots.	• Head of Cattle Handled	
1.1.2.1.4	112112	*Cattle Feedlots* Establishments primarily engaged in feeding cattle prior to slaughter and processing for human consumption.	• Head of Cattle Production	
1.1.2.1.5	11212	*Dairy Cattle Farms* Establishments primarily engaged in milking dairy cattle.	• Head of Cattle Production	
1.1.2.2	1122	*Hog and Pig Farms* Facilities primarily engaged in raising hogs and pigs, and may include farming activities, such as breeding, farrowing, and the raising of weanling pigs, feeder pigs, or market size hogs.	• Number of Hogs and Pigs • Production	
1.1.2.3	1123	*Poultry and Egg Production Farms* Facilities are primarily engaged in breeding, hatching, and raising poultry for meat or egg production. Includes chickens, turkeys, duck, geese, and others.		
1.1.2.3.1	11232, 11233, 11239	*Poultry for Meat* Establishments primarily engaged in raising poultry for meat.	• Production • Type of Poultry Raised	
1.1.2.3.2	*11231*	*Egg Production* Establishments primarily engaged in raising poultry for egg production.	• Egg Production • Poultry	
1.1.2.4	1124	*Sheep & Goat Farms* Facilities primarily engaged in raising sheep, lambs, and goats, or feeding lambs for fattening.	• Number of Sheep and Goats • Production	

ID Code	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1.1.2.5	1125	*Animal Aquaculture Facilities* Facilities primarily engaged in the farm raising of finfish, shellfish, or any other kind of animal aquaculture, and use some form of intervention in the rearing process to enhance production, such as holding in captivity, regular stocking, feeding, and protecting from predators.	• Production • Type of Fish or Shellfish Raised	
1.1.2.6	1129	*Other Farm Facilities* Facilities primarily engaged in raising animals and insects (except those identified above) such as bees, horses and other equines, rabbits and other fur-bearing animals, etc.	• Production • Type of Fish or Shellfish Raised	
1.1.3	113	**Forestry** Facilities that grow and harvest timber on a long production cycle (i.e., ten years or more). Includes forest tract operations, forest nurseries, gathering of forest products (e.g., gum and aromatic woods), and logging (i.e., cutting of trees).	• Production • Type of Forest	
1.1.4	114	**Fishing** Harvesting of fish from their natural habitats. Usually requires specialized vessels that, by the nature of their size, configuration and equipment, are not suitable for any other type of production, such as transportation. Includes fishing for finfish, shellfish, and other marine animals.	• Catch • Number of Vessels in Fleet • Type and Size of Vessel(s) • Type of Fishing	
1.2		PROCESSING/PACKAGING/PRODUCTION The transformation of livestock and agricultural products into products for intermediate or final consumption. This category is sometimes referred to as Food Manufacturing.		
1.2.1	111	**Animal Food Manufacturing** Facilities primarily engaged in manufacturing food and feed for animals from ingredients, such as grains, oilseed mill products, and meat products. These products are not intended for human consumption.		18.1.1 Animal Food Manufacturing
1.2.1.1	311119	*Farm Animal Feed Manufacturing* Manufacture of feed for cattle, hogs, pigs, poultry, aquaculture fish, and other farm animals. Includes grain and meat feed, supplements, concentrates, mixes, and other animal feed.		

ID Code	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1.2.1.1.1	311119	*On-Site Feed Mills* Establishments located at animal raising operations that produce animal feed intended primarily for local consumption.	• Production • Type of Feed Produced	
1.2.1.1.2	311119	*Off-Site Feed Mills* Establishments located apart from animal raising operations that produce animal feed intended primarily for general sale.	• Production • Type of Feed Produced	
1.2.1.2	311613	*Rendering and Meat Byproduct Manufacturing* Establishments primarily engaged in rendering animal fat, bones, and meat scraps.	• Production • Type of Rendering Done	
1.2.1.3	311111	*Pet Food Manufacturing* Manufacture of food for household pets (e.g., dogs, cats, gerbils, hamsters, aquarium fish, and others). Includes grain and meat feed, supplements, concentrates, mixes, and other pet food.	• Production • Type of Feed Produced	
1.2.2	3112	**Grain and Oilseed Milling** This industry comprises establishments primarily engaged in one or more of the following: (1) milling flour or meal from grains or vegetables; (2) preparing flour mixes or dough from flour milled in the same establishment; (3) milling, cleaning, and polishing rice; and (4) manufacturing malt from barley, rye, or other grains.		18.1.2 Grain and Oilseed Milling
1.2.2.1	31121, 31122	*Grains, Fats, and Oils Processing* Facilities engaged in milling, crushing, refining, blending, and other processing of grains, fats, and oils. Includes flour, corn, and rice milling malt, starch, vegetable fats and oils manufacturing soybean and other oilseed processing and fats and oils processing. Products are used primarily as ingredients.	• Production • Type of Product Processed	
1.2.2.2	31123	*Breakfast Food Manufacturing* Manufacture of breakfast cereal foods. Products intended for final consumption.	• Production • Type of Product Produced	

ID Code	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1.2.3	3113	**Sugar and Confectionery Product Manufacture** This industry group comprises (1) establishments that process agricultural inputs, such as sugarcane, beet, and cacao, to give rise to a new product (sugar or chocolate) and (2) those that begin with sugar and chocolate and process these further.		18.1.3 Sugar and Confectionery Product Manufacture
1.2.3.1	31131	*Sugar Manufacturing* Facilities primarily engaged in manufacturing raw sugar, liquid sugar, and refined sugar from sugarcane, raw cane sugar and sugar beets.	• Production • Type of Product Produced	
1.2.3.2	31132, 31133, 31134	*Confectionery Manufacturing* Establishments primarily engaged in manufacturing confectioneries. Includes chocolate and non-chocolate confectioneries.	• Production • Type of Product Produced	
1.2.4	3114	**Fruit/Vegetable Preserving, Specialty Food Manufacturing Facilities** This industry comprises establishments primarily engaged in manufacturing canned, pickled, and dried fruits, vegetables, and specialty foods. Establishments in this industry may package the dried or dehydrated ingredients they make with other purchased ingredients. Examples of products made by these establishments are canned juices; canned baby foods; canned soups (except seafood); canned dry beans; canned tomato-based sauces, such as catsup, salsa, chili, spaghetti, barbeque, and tomato paste; pickles; relishes; jams and jellies; dried soup mixes and bullions; and sauerkraut.		18.1.4 Fruit/ Vegetable Preserving, Specialty Food Manufacturing Facilities
1.2.4.1	31141	*Frozen Food Manufacturing Facilities* Facilities primarily engaged in manufacturing frozen fruit, frozen juices, frozen vegetables, and frozen specialty foods (except seafood), such as frozen dinners, entrees, and side dishes, frozen pizza, frozen whipped toppings, and others.	• Production • Type of Product Produced	

ID Code	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1.2.4.2	31142	*Fruit and Vegetable Canning, Pickling, Drying* Facilities primarily engaged in manufacturing canned, pickled, and dried fruits, vegetables, and specialty foods, and may package the dried or dehydrated ingredients they make with other purchased ingredients. Examples of products made in these facilities are canned juices canned baby foods canned soups (except seafood) canned dry beans canned tomato-based sauces, pickles, relishes, jams and jellies, dried soup mixes and bullions, and others.	• Production • Type of Product Produced	
1.2.5	3115	**Dairy Product Manufacturing** Facilities primarily engaged in manufacturing dairy products from raw milk and/or processed milk products; manufacturing dairy substitutes from soybeans and other nondairy substances; and manufacturing dry, condensed, concentrated, and evaporated dairy and dairy substitute products.		18.1.5 Dairy Product Manufacturing
1.2.5.1	311511	*Fluid Milk Manufacturing* Facilities primarily engaged in manufacturing processed milk products, such as pasteurized milk or cream and sour cream, and/or manufacturing fluid milk dairy substitutes from soybeans and other nondairy substances.	• Production • Type of Product Produced	
1.2.5.2	311512, 311513, 311514	*Other Non-Frozen Dairy Product Manufacturing* Facilities engaged in manufacturing butter; cheese; and dry, condensed, evaporated dairy products.	• Production • Type of Product Produced	
1.2.5.3	31152	*Ice Cream and Frozen Dessert Manufacturing* Establishments primarily engaged in manufacturing ice cream, frozen yogurts, frozen ices, sherbets, frozen tofu, and other frozen dairy desserts.	• Production • Type of Product Produced	
1.2.6	3116	**Animal Slaughtering and Processing Facilities** Establishments primarily engaged in slaughtering animals, preparing processed meats and meat byproducts, and rendering and/or refining animal fat, bones, and meat scraps. Includes establishments primarily engaged in assembly cutting and packing of meats (i.e., boxed meats) from purchased carcasses.		18.1.6 Animal Slaughtering and Processing Facilities

ID Code	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1.2.6.1	311611, 311612, 311613	*Non-Poultry Animal Slaughtering and Processing* Includes facilities for processing beef, hogs, pigs, lamb, and other such animals.	• Production • Type of Product Produced	
1.2.6.2	311615	*Poultry Slaughtering and Processing* Includes facilities for processing chickens, ducks, geese, turkeys, and other small game.	• Production • Type of Product Produced	
1.2.7	3117	**Seafood Product Processing** This industry comprises establishments primarily engaged in one or more of the following: (1) canning seafood (including soup); (2) smoking, salting, and drying seafood; (3) eviscerating fresh fish by removing heads, fins, scales, bones, and entrails; (4) shucking and packing fresh shellfish; (5) processing marine fats and oils; and (6) freezing seafood. Establishments known as "floating factory ships" that are engaged in the gathering and processing of seafood into canned seafood products are included in this industry.		18.1.6 Seafood Product Processing
1.2.7.1	311711	*Seafood Canning* Facilities primarily engaged in canning seafood (including soup) and marine fats and oils and/or smoking, salting, and drying seafood.	• Production • Type of Product Produced	
1.2.7.2	311712	*Fresh and Frozen Seafood Processing* Facilities primarily engaged in eviscerating fresh fish by removing heads, fins, scales, bones, and entrails shucking and packing fresh shellfish; manufacturing frozen seafood; and processing fresh and frozen marine fats and oils.	• Production • Type of Product Produced	
1.2.8	3118	**Bakery Products Manufacturing** Establishments producing bakery products. Includes breads, cakes, cookies, crackers, pastas, tortillas, flour mixes, and similar products.	• Production • Type of Product Produced	18.1.7 Bakery Products Manufacturing

ID Code	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1.2.9	3119	**Other Food Manufacturing** This industry group comprises establishments primarily engaged in manufacturing food (except animal food; grain and oilseed milling; sugar and confectionery products; preserved fruit, vegetable, and specialty foods; dairy products; meat products; seafood products; and bakeries and tortillas). The industry group includes industries with different production processes, such as snack food manufacturing; coffee and tea manufacturing; concentrate, syrup, condiment, and spice manufacturing; and, in general, an entire range of other miscellaneous food product manufacturing.		18.1.8 All Other Food Manufacturing
1.2.9.1	31191	*Snack Food Manufacturing* Establishments primarily engaged in salting, roasting, drying, cooking, or canning nuts processing grains or seeds into snacks; manufacturing peanut butter; and manufacturing potato chips, corn chips, popped popcorn, pretzels (except soft), pork rinds, and similar snacks.	• Production • Type of Product Produced	
1.2.9.2	31192	*Coffee and Tea Manufacturing* Establishments primarily engaged in roasting coffee; manufacturing coffee and tea concentrates (including instant and freeze-dried); blending tea; manufacturing herbal tea; and manufacturing coffee extracts, flavorings, and syrups.	• Production • Type of Product Produced	
1.2.9.3		*All Other Food Manufacturing* Includes condiments, spices, syrups, and other food products.	• Production • Type of Product	
1.2.10	312	**Beverage Manufacturing** Industries in the Beverage Manufacturing subsector manufacture beverage products. The industry group, Beverage Manufacturing, includes three types of establishments: (1) those that manufacture nonalcoholic beverages, (2) those that manufacture alcoholic beverages through the fermentation process, and (3) those that produce distilled alcoholic beverages. Ice manufacturing, while not a beverage, is included with nonalcoholic beverage manufacturing because it uses the same production process as water purification.		18.2 Beverage Manufacturing
1.2.10.1	31211	*Soft Drink Manufacturing* Establishments primarily engaged in manufacturing soft drinks; manufacturing ice; and purifying and bottling water.	• Production • Type of Product Produced	

ID Code	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1.2.10.2	312113	*Ice Manufacturing* Establishments primarily engaged in manufacturing soft drinks, manufacturing ice, and purifying and bottling water.	• Production	
1.2.10.3		*Alcoholic Beverage Manufacturing* Establishments primarily engaged in manufacturing alcoholic beverages.		
1.2.10.3.1	31212	*Breweries* Establishments primarily engaged in brewing beer, ale, and malt liquors.	• Production • Type of Product Produced	
1.2.10.3.2	31213	*Wineries* Establishments primarily engaged growing grapes and manufacturing wine and brandies, manufacturing wine and brandies from grapes and other fruits grown elsewhere, and blending wines and brandies.	• Production • Type of Product Produced	
1.2.10.3.3	31214	*Distilleries* Establishments primarily engaged in distilling potable liquors, distilling and blending liquors, and blending and mixing liquors and other ingredients.	• Production • Type of Product Produced	
1.2.11	3122	**Tobacco Product Manufacturing** Establishments engaged in the stemming and re-drying of tobacco and the manufacture of tobacco products, including cigarettes, cigars, pipe tobacco, and similar products.	• Production • Type of Product Produced	
1.3		**AGRICULTURAL AND FOOD PRODUCT STORAGE** Establishments engaged in operating warehousing and storage facilities for agricultural and food products. These establishments provide facilities to store goods. They do not sell the goods they handle. These establishments take responsibility for storing the goods and keeping them secure. They may also provide a range of services, often referred to as logistics services, related to the distribution of goods.		

ID Code	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1.3.1	49313	**Bulk Food Storage Facilities** Establishments primarily engaged in operating warehousing and storage facilities for bulk food (e.g., grains, unprocessed vegetables and fruits). Includes grain elevators. Facilities may be unrefrigerated or refrigerated.		
1.3.1.1	493130	*Grain Elevators* Facilities for storing large quantities of grains. Generally located in farming areas and receive grain from several farms.	• Product(s) Stored • Storage Capacity	
1.3.1.2	493130	*Non-Refrigerated Bulk Food Storage Facilities* Facilities for storing bulk farm products (e.g., vegetables and fruits) in unrefrigerated areas.	• Product(s) Stored • Storage Capacity	
1.3.1.3	493120	*Refrigerated Bulk Food Storage Facilities* Facilities for storing bulk farm products in refrigerated areas.	• Product(s) Stored • Storage Capacity	
1.3.2		**Processed Food Storage Facilities** Establishments primarily engaged in operating warehousing and storage facilities for processed foods, either intermediate or finished products. Facilities may be unrefrigerated or refrigerated.	• Product(s) Stored • Refrigerated • Storage Capacity • Type of Facility • Unrefrigerated	
1.3.2.1	493130	*Non-Refrigerated Processed Food Storage Facilities* Facilities for storing processed food products in unrefrigerated areas.	• Product(s) Stored • Storage Capacity	
1.3.2.2	493120	*Refrigerated Processed Food Storage Facilities* Facilities for storing processed food products in refrigerated areas.	• Product(s) Stored • Storage Capacity	
1.4		**AGRICULTURAL AND FOOD PRODUCT TRANSPORTATION** Establishments engaged in transporting agricultural and food products. These establishments provide facilities to store goods.		

ID Code	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1.4.1	484	**Road Transport of Agricultural and Food Products** This category includes transportation facilities (e.g., trucks, truck terminals, truck wash and disinfection facilities, highways, bridges, and tunnels) involved in the transport of agricultural and food products by truck.	• Products Transported • Quantity	
1.4.2	482	**Rail Transport of Agricultural and Food Products** This category includes transportation facilities (e.g., rail tank cars, rail car loading/unloading terminals, rail car wash and disinfection facilities, rail rights-of-way, railroad bridges, and railroad tunnels) involved in the transport of agricultural and food products by rail.	• Products Transported • Quantity	
1.4.3	483	**Maritime Transport of Agricultural and Food Products** This category includes transportation facilities (e.g., barges, loading/unloading piers, waterways, canals and locks, and ports) involved in the transport of agricultural and food products by water.	• Products Transported • Quantity	
1.4.4	481	**Air Transport of Agricultural and Food Products** This category includes aviation facilities (e.g., aircraft and airports) involved in the transport of agricultural and food products by air.	• Products Transported • Quantity	
1.5		**AGRICULTURAL AND FOOD PRODUCT DISTRIBUTION** Wholesale and retail distribution of agricultural and food products.		
1.5.1	4245	**Farm Product Wholesalers** Establishments primarily engaged in the merchant wholesale distribution of agricultural products, such as grains; field beans, livestock, and other farm product raw materials (excluding seeds).		
1.5.1.1	42451	*Grain and Field Bean Wholesalers* Establishments primarily engaged in the merchant wholesale distribution of grains; such as corn; wheat; oats; barley; unpolished rice, dry beans, and soybeans; and other inedible beans.	• Products Wholesaled • Quantity	
1.5.1.2	42452	*Livestock Markets* Establishments that receive, hold, and sell livestock (cattle, sheep, swine, horses, llamas, bison, etc.) to all entities within the production chain (from ranchers, to backgrounders, to feedlots) and to processing (slaughter) facilities.	• Livestock Marketed • Quantity	

ID Code	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1.5.1.3	42459	*Other Farm Product Wholesalers* Establishments primarily engaged in the merchant wholesale distribution of other farm products.	• Products Wholesaled • Quantity	
1.5.2		**Grocery and Related Product Wholesalers** Establishments primarily engaged in the merchant wholesale distribution of a general line (wide range) of groceries. Includes general line groceries, packaged frozen foods, dairy products, poultry products, confectionaries, fish and seafood products, meat and meat products, fresh fruits and vegetables, and others.	• Products Wholesaled • Quantity	
1.5.3	445	**Food and Beverage Retailers** Establishments retailing food and beverages merchandise from fixed point-of-sale locations. Generally have special equipment (e.g., freezers, refrigerated display cases, and refrigerators) for displaying food and beverage goods. Generally have staff trained in the processing of food products to guarantee the proper storage and sanitary conditions required by regulatory authority.		
1.5.3.1	44511	*Supermarkets and Grocery Stores* Establishments generally known as supermarkets and grocery stores primarily engaged in retailing a general line of food, such as canned and frozen foods; fresh fruits and vegetables; and fresh and prepared meats, fish, and poultry. Included are delicatessen-type establishments primarily engaged in retailing a general line of food.	• Chain Supermarket • Independent Market Location Outside Metropolitan Area • Sales Volume • Store Size • Suburban • Type of Store • Urban	
1.5.3.2	44512	*Convenience Stores* Establishments known as convenience stores or food marts primarily engaged in retailing a limited line of goods that generally includes milk, bread, soda, and snacks. May be located at motor vehicle refueling stations.	• Chain Supermarket • Independent Market Location Outside Metropolitan Area • Sales Volume • Store Size • Suburban • Type of Store • Urban	

ID Code	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1.5.3.3	4452	*Specialty Food Stores* Establishments primarily engaged in retailing specialized lines of food. Includes meat markets, fish and seafood markets, fruit and vegetable markets, baked goods stores, and others.	• Chain Supermarket • Independent Market Location Outside Metropolitan Area • Sales Volume • Store Size • Suburban • Type of Store • Urban	
1.5.3.4	4453	*Beer, Wine, and Liquor Stores* Establishments primarily engaged in retailing packaged alcoholic beverages, such as ale, beer, wine, and liquor.	• Chain Supermarket • Independent Market Location Outside Metropolitan Area • Sales Volume • Store Size • Suburban • Type of Store • Urban	
1.5.4	722	**Food Service and Drinking Facilities** Facilities preparing meals, snacks, and beverages to customer order for immediate on-premises and off-premises consumption.		
1.5.4.1	7221	*Full Service Restaurants* Establishments primarily engaged in providing food series to patrons who order and are served while seated (i.e., waiter and waitress service) and pay after eating. May also provide other services, such as takeout services. May be stand-alone facilities or may be attached to another facility (e.g., hotel).	• Location • Patron Capacity • Patron Volume • Recreational Area • Rural • Suburban Urban–Downtown • Urban–Other	

ID Code	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1.5.4.2	7222	*Limited Service Food Facilities* Establishments primarily engaged in providing food services where patrons generally order or select items and pay before eating. Most establishments do not have waiter/waitress service. Includes carry out restaurants, delicatessen restaurants, fast food restaurants, pizzerias, sandwich shops, cafeterias, snack bars, ice cream stands, doughnut shops, mobile food service vehicles, and similar facilities.	• Location • Patron Capacity • Patron Volume • Recreational Area • Rural • Suburban • Urban–Downtown • Urban–Other	
1.5.4.3	72241	*Drinking Establishments* Facilities primarily engaged in preparing and serving alcoholic beverages for immediate consumption. May also provide limited food services.	• Location • Patron • Capacity Patron • Recreational Area • Rural • Suburban • Urban-Downtown • Urban-Other	
1.5.4.3.1	722410	*Bars* Facilities serving alcoholic beverages generally with no or limited live entertainment. Includes bars, taverns, and cocktail lounges.	• Location • Patron • Capacity Patron • Recreational Area • Rural • Suburban • Urban-Downtown • Urban-Other	
1.5.4.3.2	722410	*Nightclubs* Facilities serving alcoholic beverages and with regular live entertainment and/or dancing.	• Location • Patron • Capacity Volume • Recreational Area • Rural • Suburban • Urban-Downtown • Urban-Other	

ID Code	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1.5.4.3.3	722410	*Nightclub Districts* Areas in which there is a concentration of nightclubs, and related facilities.	• Location • Number of Nightclubs and related Facilities in District • Patron Capacity • Patron Volume • Recreational Area • Rural • Suburban • Urban-Downtown • Urban Other	
1.6		**AGRICULTURE AND FOOD SUPPORTING FACILITIES** Facilities providing supporting services in agriculture and food.		
1.6.1	3253	**Agricultural Chemical Manufacture** Includes fertilizers, pesticides, and other chemicals.		
1.6.2	325412	**Veterinary Pharmaceutical Manufacture** Establishments engaged in the manufacture of pharmaceuticals for use in animals.	• Production • Type of Pharmaceuticals Manufactured	10.4.3.1 Pharmaceutical Manufacturing Facilities
1.6.3	42491	**Farm Supply Wholesalers** Establishments primarily engaged in the merchant wholesale distribution of farm supplies, such as animal feeds, fertilizers, agricultural chemicals, pesticides, plant seeds, and plant bulbs.	• Sales Volume • Type of Supplies Wholesaled	
1.6.4	4442	**Farm Supply Retailers** Establishments primarily engaged in retailing farm supplies.	• Sales Volume • Type of • Supplies Retailed	
1.6.5	54194	**Veterinary Services** Establishments engaged in the practice of veterinary medicine, dentistry, or surgery for animals.	• Case Load • Type of Animals Treated	
1.6.6	541712	**Agricultural Testing Laboratories** Establishments conducting soil, seed, plant, animal, and related testing.	• Case Load • Type of Testing Done	

ID Code	NAICS Code	Description	Attributes Of Interest	Other Categorization(s)
1.6.7	541712	**Agricultural and Food Research** Establishments engaged in conducting research and experimental development in agriculture and food sciences.	• Number of Employees on Site • Type of Research Done	
1.7		**REGULATORY, OVERSIGHT, AND INDUSTRY ORGANIZATIONS** Organizations that provide technical, operation, pricing, and business oversight and support to the Agriculture and Food Sector.		
1.7.1	921110	**Federal Agriculture and Food Agencies** Federal agencies that deal with the agriculture and food system, including USDA, FDA, and others. Includes Federal extension services.	• Number of Employees at Site	
1.7.2	921110	**State, Local, Regional Agriculture and Food Agencies** State, local, and regional agencies dealing with agriculture and food in their jurisdiction, including public health departments, agricultural extension services, and others.	• Number of Employees at Site	
1.7.3		**Agriculture and Food Industry Organizations** Industry organizations (e.g., farmers associations, ranchers associations, etc.) that provide industry-wide support.	• Number of Employees at Site	
1.7.4		**International Agriculture and Food Organizations** International organizations dealing with agriculture and food issues.	• Number of Employees at Site	
1.8	**2122**	**OTHER AGRICULTURE AND FOOD** Agriculture and Food facilities not elsewhere classified.		


FDA
Food and Drug
Administration


USDA


Homeland
Security