NATIONAL CENTER FOR
FOOD PROTECTION AND DEFENSE
A HOMELAND SECURITY CENTER OF EXCELLENCE

March 10, 2013

NCFPD Response to the NIST RFI for:

Developing a Framework To Improve Critical Infrastructure Cybersecurity

The National Center for Food Protection and Defense (NCFPD), a U.S. Department of Homeland Security (DHS) Center of Excellence founded in 2004, is at the forefront in developing and implementing new risk management approaches within the Food and agriculture Sector. NCFPD is an active contributor to the functions of the Food and Agriculture Sector Coordinating Councils and Government Coordinating Council, whose primary mission is protecting the nation's food system from all risks. NCFPD's consortium of investigators, partners, and stakeholders come from the private sector, national laboratories, universities, centers of excellence, and international non-governmental organizations. It is this breadth of stakeholders and partners that enable NCFPD to understand current food vulnerabilities and provide potential solutions. NCFPD conducts research aimed at protecting the nation's food supply by incorporating stakeholder feedback in research, broad outreach, and a rigorous peer review process. NCFPD developed novel tools to conduct risk assessment for the entire sector such as the Food and agriculture Sector Criticality Assessment Tool (FASCAT). FASCAT was deployed to the states in 2009, in partnership with the state and private sectors, to identify critical components of state food supply chains. To date, there are 741 food commodity specific assessments conducted. This process includes assessment of cyber threats and their potential consequences. These data indicate private sector concern with the security of their supervisory control and data acquisition systems (SCADA), information storage, and authentication and authorization systems. Additionally, NCFPD was a direct contributor to the last three national Bio-Terrorism Risk Assessments, conducted in collaboration between DHS, the U.S. Department of Agriculture (USDA) and the Food and Drug Administration (FDA). These assessments reflected the overall cyber risks to the nation's food supply.

NCFPD prepared written guidance to develop sector specific cyber defense plans and cyber training. These documents, in development for more than a year, offer specific guidance to small and medium sized firms within the food and agriculture sector, and provides resources to enhance their cyber security. This effort built on the experience and operational insight gained through the FASCAT process. NCFPD is developing a new, private sector specific, risk analysis tools for the sector which will include cyber risks and the potential consequences of a cyber-defense failure or the compromise of a critical SCADA system.

NCFPD has a unique perspective based upon eight years of experience in the food and agriculture sector, academia, industry, and the government. **Therefore, NCFPD respectfully submits information, observations, and recommendations to assist NIST with its critical tasks under *Executive Order 13636:***

1. Sector Overview from a Cyber Perspective

The global food system is the most complicated supply chain known. It comprises thousands of farms and hundreds of thousands of food processors, distributors, and retail establishments. The majority of food firms are small and employ few people but which employ cyber technologies at varies levels of sophistication and complexity. The food system, from primary production to final consumption, was optimized to deliver a wide array of foods from around the world at the lowest possible cost. Because it is a vast system comprised of buyers and sellers, where bidding for business is the rule, there is great reluctance to share proprietary or intellectual property, even when firms are forced to collaborate on food safety. The nation's food system was not designed for resilience against intentional disruption or contamination, and the existing information systems do not make optimization feasible. The diversity of functions, processes, and supply chain components present unique challenges to management. Consequently, the complexity and diversity of the supply chains necessitates the use of cyber systems at all levels within the infrastructure from farm operations to retail.

Indeed, nearly every aspect of food production in the U.S. employs some facet of cyber technologies. From farms to food retailers, the Internet enables a means of coordination, collaboration, financial transactions, and is now a vital component of daily operations. There are five distinct cyber system environments within the Food & Agriculture sector and each involves information management, SCADA systems, and quality assurance / quality control (QA/QC):

1. Pre-Harvest production support systems;
2. Harvest systems;
3. Transportation systems;
4. Food Processing control systems;
5. Food product distribution and tracking systems.

We depend upon computer networks to link each supply-chain system together (e.g. animal operations, harvesting, processing, shipping and distribution, imports, and exports). Technology systems are routinely linked to expedite work and increase efficiency. Materials sourcing, shipping and receiving, import and export operations, processing facilities, warehouse operations, and distribution are linked and integrated via the Internet within food production operations. Further, mobile devices and home computers are routinely used to control SCADA systems and conduct other work functions from home. If you examine modern food processing operations (e.g., fluid milk plant) process management is computer controlled (i.e., quality assurance, safety, and testing protocols). Combined with the use of systems to manage staff assignments, work hours, and worker qualification and recurrent training, staffing and HR functions are integrated with our process control systems. The food and agriculture sector's cyber infrastructure supports financial transactions, energy, facility management, and SCADA systems.

The new FDA Food Safety Modernization Act (FSMA) has new requirements for record keeping and for assuring rapid access to timely and accurate product processing and distribution information. These new requirements assume the use of advanced information technologies (IT). Therefore, it is imperative these firms have appropriate cyber defense systems to ensure high availability and reliability of their IT systems.

2. Current Cyber Risk profile for the Food and Agriculture Sector

Cybercrime is a growing threat to our own privacy and every critical infrastructure. This is particularly true for the nation's food and agriculture sector. According to the 2012 Global Security Report, recently issued by Trustwave, the food and beverage industry was the most targeted industry in 2010 accounting for 44% of the 300 major cyber breaches investigated by Trustwave. Moreover, food and beverage franchisees have similar networks that offer hackers "a formulaic blueprint for fleecing a large number of victims".[1] Since criminals and activists employ illegal cyber activities to disrupt, gain access to, and steal information from the private sector and government within the food and agriculture sector, cyber security is increasingly important to the sector.

The retail component of the sector is not the only attractive target for cybercrime. For a variety of motivations, ranging from political to ideology to profit, the sector is a poorly defended cyber environment. The passage of FSMA in 2011 assigns additional responsibilities to owners and operators of the nation's food and agriculture sector; cyber security efforts must be included in these new responsibilities to harden our food supply chains against intentional and unintentional threats. The new requirements for record keeping, product tracing and supply chain documentation compel the sector to keep digital records and cyber technology-based supply chain management and SCADA systems. These systems must be reliable and secure if they are to comply with the new FSMA requirements.

Many cyber systems within the food and agriculture sector employ the Internet to connect to other interdependent infrastructures systems within our nation and across the globe (e.g. water systems, energy, financial and transportation systems). The Internet is a global system linking small rural towns to every major city in the world.

There are a variety of risks to food systems, and each new technological development brings new foreseen and unforeseen risks. The consequences of cyber-attacks on the food system is constantly increasing with the global expansion of the food supply chain, the rate of product movement through the supply chain, and the growth of the scale and complexity of food system. Reliable cyber technologies are necessary to prevent crippling cyber-attacks. We rely on these systems to investigate foodborne illness outbreaks, initiate product recalls, validate suppliers and buyers, and manage Q/A programs. From a food defense perspective, there are numerous drivers threatening our food supply. These drivers include: public health surveillance system functionality, the food systems' complexity, and conducting trade with global partners that operate in high-risk areas (e.g., Egypt and the Ivory Coast). Specific intentional cyber threats include: economically motivated adulteration (EMA), presence of disgruntled employees, criminal activity and organized crime, and potential targeting of the food system by terrorist organizations.

One example of cyber technology exploitation in intentional acts is EMA. EMA activities routinely employ the Internet to identify sales and distribution opportunities for the fake or adulterated products via the Internet. Furthermore, attackers steal and take advantage of key process knowledge to exploit and dupe technology-based quality and safety testing systems. Recent examples include the use of melamine in milk products and to create fake wheat gluten sold via Internet based transactions. While EMA is not defined as terrorism, it is criminal. EMA is not intended to cause public health harm as casualties reduce the potential for profit, but perpetrators of EMA do not necessarily consider or understand the dangers (e.g., the melamine contamination events in China). These recent EMA events demonstrate evasion of private sector quality assurance systems, government inspection, and surveillance systems. If adulteration for profit is achievable, so is adulteration for harm.

[1] 2012 Global Security Report, www.Trustwave.com

Due to the frequency and consistency of cyber-attacks that occur on a continual basis, it is conceivable that cyber-attacks will continue and expand. Cyber threats to our community organizations and to the national food system can vary. But most fall into two basic categories:

1. The theft of, obstruction of access to, alteration of, or destruction of critical data stored on these systems; and,
2. The threat to a cyber-based control system where a person(s) attempts unauthorized access to a control system device and/or network using a data communications pathway with the intent of influencing the functioning of that control, disabling it, or preventing authorized access to it.

There are numerous examples of cyber threats with dramatic and traumatic results. Cyber threats can damage brands, shut down plants, cause job and financial losses, and result in human illness or death. Hackers and adversaries can employ malicious code or malware, to disrupt operations, to cover criminal actions, or to actively seek financial gain. The impact of cyber-attacks to food sector can be catastrophic. Many of the significant cyber worms now employed by hackers are designed to steal sensitive information (e.g., financial transactions, personal information, passwords).

Unfortunately, cyber attackers are very adept at circumventing traditional defenses (e.g., anti-virus software, intrusion detection software, and firewalls). Even encrypted web transactions may not protect sensitive information. Malware writers are easily circumventing basic security controls. Therefore, the food sector needs to increase cyber security awareness to mitigate cyber threats. Cyber attackers are creative, driven, adaptable, and opportunistic. They intend mayhem, mischief, make political statements, and are capable of causing physical and financial harm. Cyber attackers employ sophisticated tools, advanced malware, social skills, and basic psychology to meet their objectives, which includes data theft, product tampering, and direct attacks on the nation's food system.

3. NCFPD Recommendations for Food and agriculture Sector Specific Cyber Defense Framework

Given the complexity and diversity of food and agricultural systems, it is imperative that any effort at a national sector-specific and cross-sector cyber defense framework, and its supporting guidance, be flexible, adaptable, scalable, repeatable, and cost effective. With slim profit margins (i.e., 2%) any deployable solution must increase profitability. This presents a unique challenge to the food sector; any approach to mitigate the cyber threat must focus on risk assessment tools, protective policies, and industry best practices that contribute to food system availability, reliability, safety, and profitability. The selected approach also must enhance financial security, reduce insurance risks, and aid in improving overall company performance. The food and agriculture sector must broadly adopt general and sector specific information security and cyber defense standards and best practices

Proposed NIST Framework Issues:

- *A consultative process to assess the cyber security-related risks to organizational missions and business functions.*

NCFPD uses FASCAT as a model for collaborative assessment. This tool is now broadly used in the U.S. within the food and agriculture sector. Building on this established approach within the sector was key to the new CRIticality and SpaTial AnaLysis (CRISTAL) risk assessment tool, and must be a foundation for any new national cyber defense framework. CRISTAL enables industry to identify risks and objectively quantify these risks with the intent to share data among the food and agriculture sector supply chain partners and collaborators in a non-threatening manner. CRISTAL's collaboration must extend beyond internal company components, and must include suppliers, all levels of government, and government or industry sanctioned regulators. While proprietary requirements, intellectual property imperatives, and trade rules must be adhered to at all times, suppliers and customers must be integrated into risk assessment and risk mitigation programs to protect the entire supply chain. Furthermore, adoption of and adherence to IT system protection and secure data exchange standards are key to financial and food system security. The FDA, USDA, and public health inspection components must be integrated with cyber security standards to meet record keeping requirements within the SCADA and distribution management systems to ensure data reliability and availability.

- *A menu of management, operational, and technical security controls, including policies and processes, available to address a range of threats and protect privacy and civil liberties;*

An adaptable and flexible range of cyber system solutions must be available. The protective needs and scale of cyber defense systems will vary with the size of the firm their IT systems. The food and agriculture sector is composed of large and small firms, some with only one or two employees. While all may use some form of IT support for their operational, management, and record keeping requirements, their cyber defense needs will vary from a single desktop computer to a vast array of information management and SCADA systems. The range of threats varies, but often unauthorized access to a large firm's IT infrastructure can be accomplished by compromising a small suppliers IT systems thereby exploiting its access to the larger firm's systems. Therefore, standards, protocols, system monitoring and training collaboration must extend across food systems to supporting infrastructures (e.g., transportation, energy and water).

- *A consultative process to identify the security controls that would adequately address assessed risks*[8] *and to protect data and information being processed, stored, and transmitted by organizational information systems;*

Once the initial risk assessment process is complete, employing tools like CRISTAL and FASCAT, a wide range of best practices, cyber security controls and protocols are already available to address identified system risks. The challenge is the tailoring of certain of these protective approaches to the unique nature of the food supply chain and then the broad sharing of information on these security controls and protocols; availability, employment, limitations and maintenance must be accomplished. Additionally, there must be broad sector support to collaboratively integrate these protective measures across the supply chains and to provide training and deployment standards / best practices. To facilitate this, regulatory bodies must adopt supporting regulations and guidelines in support of this effort.

- *Employ metrics, methods, and procedures used to assess and continuously monitor the effectiveness of security controls. The controls are selected and deployed in organizational information, finance and industrial management systems. Finally, available processes can be used to facilitate continuous improvement in such controls;*

The use of metrics in monitoring best practices and food safety is widely accepted within the food and agriculture sector. If successful and cost effective cyber defense frameworks, cyber controls, and system monitoring are developed, sector adoption will not be technically difficult. With the myriad of new food safety rules and regulations now promulgated by FDA and USDA, the regulatory, best practice, and varied industry standards potentially can drown out information sharing efforts. Any proposed cyber defense framework must take into consideration the complex but cluttered food system environment.

- *Create a comprehensive risk management approach that provides the ability to assess, respond to, and monitor information security-related risks and provide senior leaders/executives with the necessary information to help them make ongoing risk-based decisions;*

NCFPD created a sector-specific approach to risk assessment that is highly collaborative, yet supply chain specific. The food sector has a long established food handling and safety protocol, Hazard Analysis of Critical Control Points (HACCP), based upon commodity specific standards, protocols, and supply chain collaboration. This model is well established and validated within the food and agriculture sector. This foundation should be extended within the sector to enable sector firms to cooperatively implement cyber security standards and protocols to protect each firm within the supply chain from cyber intrusion and exploitation.

- *Provide a menu of privacy controls to protect privacy and civil liberties.*

Any proposed cyber security framework must protect individual privacy, intellectual property, proprietary process information, and market data of the firms and supply chain partners adopting the standards, protocols, protective controls and security system monitoring systems.

In response to the specific questions in the Request For Information cited above, NCFPD offers the following input and observations for consideration as NIST develops the proposed *Cyber Security Framework*:

Current Risk Management Practices

1. *What do organizations see as the greatest challenges in improving cyber security practices across critical infrastructure?*

NCFPD found two key areas for mid and small-sized firms that impact deployment of effective cyber security. First, most mid- and small-sized firms do not have dedicated cyber security specialists. They rely upon the traditional operations staff within their IT department or upon a specific manager within the firm. Second, there are often contracted IT personnel not focused on the overall interaction of the firm within a larger supply chain, but instead focused on insuring the firm's IT systems are functional only for conducting business transactions. They provide little or no assistance with training all the firm's staff in optimal cyber security practices. Moreover, any security monitoring provided is limited and focuses on narrow contracted tasks. Because most managers do not perceive the food and agriculture sector is a significant cyber target, there is often a limited awareness of the cyber risks and the need for cyber security.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based framework for critical infrastructure?

In the food and agriculture sector there is a perception that any IT collaboration between firms may compromise intellectual property or proprietary information; IT systems are seen as internal to the firm. Cross- supply chain or cross-infrastructure cyber security collaboration or coordination requires senior management focus. It also requires industry organizations to promote cyber security standards and best practices so they diffuse the threats through the supply chain component firms.

3. Describe your organization's policies and procedures governing risk generally and cyber security risk specifically. How does senior management communicate and oversee these policies and procedures?

NCFPD found current cyber security policies vary widely within the sector. While there is a strong focus on food safety risk reduction to protect their brand's reputation, regulatory requirements, and insurance stipulations, there is less focus on cyber security. Food safety risks are an understood management focus, yet cyber security is often misunderstood as senior management is not aware of the inherent risks and their significance to their operations. In a recent FASCAT assessment, it was the belief of senior management at a medium-sized food-processing firm that their IT system, data management, and SCADA systems, were not connected to the Internet. Upon further questioning, it was acknowledged that senior staff and certain operational managers could log into the firm's systems from their homes during non-duty hours to monitor firm operations! These senior managers were unaware of VPN technology and they did not employ them. This is a common posture for cyber security risks within the food and agriculture sector, particularly at the medium and small sized firms.

4. Where do organizations locate their cyber security risk management program/office?

For most medium and small firms in the food and agriculture sector, there is typically no specific cyber risk management office. Instead, this function is realized by their IT management office as an additional duty for a staff member or as a function of a senior company officer. Conversely, large, international food corporations have dedicated risk management offices tasked with investigating cyber security risks. In a few cases, there is a dedicated, separate cyber security risk management structure within the firm.

5. How do organizations define and assess risk generally and cyber security risk specifically?

Due to food safety regulatory and liability issues, most firms have some degree of risk management programs. Most often these are food safety and liability centered programs. Most are fairly sophisticated with their food safety risk programs meeting regulatory and insurance requirements. Most of these are based upon the HACCP program and are routinely inspected, monitored, and evaluated internally and externally. Hence, there is a well-developed risk management culture in the sector. Unfortunately, this culture often does not extend, with the same focus and sophistication, into the cyber risks for most medium and small-scale firms.

6. To what extent is cyber security risk incorporated into organizations' overarching enterprise risk management?

Most organizations adhere to recommended IT practices for firewalls, anti-virus, anti-malware and software patch updates; however many do not have sophisticated network monitoring systems, employee password use training and enforcement program, or cyber risk management collaboration. This level of cyber risk management culture maturity is not yet developed within much of the food and agriculture sector.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

Within the food and agriculture sector, standards vary widely. In the cases where firms contract with outside venders for cyber risk management (typically larger firms), the standards follow current IT industry best practices. While NCFPD has not surveyed firms to identify the predominant standards employed, we are working to incorporate risk assessment functions within the new CRISTAL assessment tool to provide more detailed insight into this sector's risk practices profile. What we have learned is that these standards vary widely and are customarily not based upon the best practices across firms within the sector, but rather upon the actual direct experience of the specific firm. Because the adoption of high-risk management standards and practices is experience based, if they have not experienced a significant cyber security event, they probably have an unsophisticated approach to cyber risk management.

> *8. What are the current regulations and regulatory reporting requirements in the U.S. (e.g. local, state, national, and other) for organizations relating to cyber security?*

Within the food and agriculture sector, there are few specific USDA, FDA or NOAA cyber risk related event reporting requirements; however, there are very specific production and food safety record keeping and reporting requirements. Any failure in this responsibility area, whether as the result of a clerical error, system malfunction or cyber event if it impacts consumer safety, is reportable and may be investigated by FDA. It is this all too common food production records failure event experience and the recent growth in cyber event related financial losses, where they have occurred, that currently drives existing cyber risk management within the medium and small firms. Few state-level public health agencies have cyber risk regulations or cyber risk management requirements for firms in the sector. However, USDA and FDA have published very general cyber risk practices recommendations for the sector. Unfortunately, few firms engaged in the FASCAT assessment process seemed to be aware of these, with the exception of the major firms.

> *9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?*

During the past five years, NCFPD conducted and facilitated FASCAT assessments across the sector, to identify critical components within the supply chains. The interdependency of functions, such as transportation, energy, cyber as their impact product processing, packaging and distribution was assessed on a comparative risk basis to help the firms and government understand criticality and interdependency. It was clear that IT systems are fundamental components of these supply chains and they present unique risks. Additionally, the majority of the firms participating in these assessments recognized the criticality of these systems, but most never experienced a significant cyber-attack, and therefore did not see the need for specialized and focused cyber risk management efforts beyond customary IT best practices as they understood them. When queried on what these best practices were, the response was generally limited to maintaining current software patches, maintaining firewalls, anti-virus software and using passwords access to networks. Few knew of password training for employee and the need to maintain a high level of password security or cross firm cyber security collaboration. Most, however, did see the value, if senior management saw it as cost effective and necessary. This demonstrates a significant challenge to cyber security improvement within the sector.

> *10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cyber security risk?*

Most medium and small firms in the food and agricultural sector base their cyber security risk management practices on their direct experience with cyber security events. As these events impact the level of cyber security sophistication within the firm, their goals for cyber security are increased only when there is a performance gap. These goals are rarely based upon a sector wide or a national standard.

> *11. If your organization is required to report to more than one regulatory body, what information does your organization report and what was your organization's reporting experience?*

For the food and agriculture sector, complying with regulations and reporting to multiple agencies at the state and federal levels is the norm. This places enormous administrative burdens on the management of these firms, whether large, medium, or small. Additionally, the burden of routine inspections by various health agencies at the state and local levels and regulatory "noise" is high enough that any new regulation is unwelcome and vehemently debated. Currently, the regulatory burden of cyber risk / cyber event reporting within the food and agriculture sector is very low. The standards and framework for improving overall cyber security within the sector that are adopted at the federal level must be closely coordinated via extensive collaboration with industry organizations. These standards must also leverage the current food safety risk management culture to limit resistance and to ensure the standards become a component of food safety risk management with minimal regulatory aspects. One recommended approach is to engage the industry organizations in collaboration with the sector's insurance industry and the financial community to institutionalize these standards and best practices as a part of their underwriting and risk rating functions.

> *12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cyber security conformity assessment?*

At present, NCFPD has not detected a significant visibility of international cyber risk organizations in the cyber risk practices of food and agriculture sector medium and small firms However, there are food sector specific standards and safety organizations that do have an influence with the food safety and record keeping practices of international food and agriculture firms. Given the global nature of the nation's food system and the risk of EMA, to say nothing of the potential for a direct attack on our food system, it is imperative that international standards for cyber security within the food and agriculture sector are improved and institutionalized within the international food and agriculture production and distribution communities. The insurance industry should be directly engaged in the promulgation and adoption of cyber risk management practices and programs.

Use of Frameworks, Standards, Guidelines, and Best Practices

> *1. What additional approaches already exist?*

Within the food and agriculture sector several general cyber security program approaches are published by the federal government and by state level cyber protection agencies. The following are examples of guidance provided to the private sector within the nation's food and agriculture infrastructure:

- **Food and agriculture Sector-Specific Plan**, An Annex to the National Infrastructure Protection Plan, 2010. See: http://www.dm.usda.gov/ohsec/docs/nipp-ssp-food-ag-2010.pdf

This document was a collaborative effort of government and industry and contains general non-regulatory cyber risk management guidance for the sector.

- **USDA/FSIS: "**Developing A Food Defense Plan For Meat And Poultry Slaughter And Processing Plants" January 2007 (Updated June 2008)

See: http://www.fsis.usda.gov/PDF/Food_Defense_Plan.pdf
Contains very general computer systems security practices and password controls recommendations.

- **FDA** online food defense guidance document that provides general cyber security information at: http://www.fda.gov/downloads/Training/ForStateLocalTribalRegulators/UCM218900.pdf

- **FDA:** Guidance for Industry: Food Producers, Processors, and Transporters: Food Security Preventive Measures Guidance,

See:http://www.fda.gov/Food/GuidanceComplianceRegulatoryInformation/GuidanceDocuments/FoodDefenseandEmergencyResponse/ucm083075.htm
This document provides general computer security guidance for food sector firms.

- Overview of Cyber Vulnerabilities, U.S. Department of Homeland Security, 2005

- Control Systems Security Program (CSSP), U.S. Department of Homeland Security, 2005

- Recommended Practice: Improving Industrial Control Systems CyberSecurity with Defense-In-Depth Strategies, U.S. Department of Homeland Security, US-CERT October 2009 (Numerous additional useful resources are listed at the end of this document)

- Strategy for Securing Control Systems, Coordinating and Guiding Federal, State and Private Sector Initiatives, U.S. Department of Homeland Security, October 2009

- Malware Threats and Mitigation Strategies, US-CERT Informational Whitepaper, May 16, 2005, Produced by the Multi-State Information Sharing and Analysis Center and the U.S. Computer Emergency Readiness Team.

- Common Cybersecurity Vulnerabilities in Industrial Control Systems, U.S. Department of Homeland Security, May 2011
- SCADA Systems and the Terrorist Threat: protecting the Nation's Critical Control Systems, Testimony before the Subcommittee on Economic Security, Infrastructure Protection and CyberSecurity and the Subcommittee on Emergency Preparedness, Science and Technology of the Committee on Homeland Security, US House of Representatives, One Hundred Ninth Congress, October 18, 2005 by the Federation of American Scientist.

- Several states operate cyber security guidance via state operated websites. These guidance sources are used by some firms within the sector for developing internal cyber risk management programs. See:
  - http://www.dhses.ny.gov/ocs/resources/

- http://www.iso.scio.nc.gov/

2. Which of these approaches apply across sectors?

- Overview of Cyber Vulnerabilities, U.S. Department of Homeland Security, 2005
- Control Systems Security Program (CSSP), U.S. Department of Homeland Security, 2005
- Recommended Practice: Improving Industrial Control Systems CyberSecurity with Defense-In-Depth Strategies, U.S. Department of Homeland Security, US-CERT October 2009 (Numerous additional useful resources are listed at the end of this document)
- Strategy for Securing Control Systems, Coordinating and Guiding Federal, State and Private Sector Initiatives, U.S. Department of Homeland Security, October 2009
- Malware Threats and Mitigation Strategies, US-CERT Informational Whitepaper, May 16, 2005, Produced by the Multi-State Information Sharing and Analysis Center and the U.S. Computer Emergency Readiness Team.
- Common Cybersecurity Vulnerabilities in Industrial Control Systems, U.S. Department of Homeland Security, May 2011
- SCADA Systems and the Terrorist Threat: protecting the Nation's Critical Control Systems, Testimony before the Subcommittee on Economic Security, Infrastructure Protection and CyberSecurity and the Subcommittee on Emergency Preparedness, Science and Technology of the Committee on Homeland Security, US House of Representatives, One Hundred Ninth Congress, October 18, 2005 by the Federation of American Scientist.

- http://www.dhses.ny.gov/ocs/resources/
- http://www.iso.scio.nc.gov/

3. Which organizations use these approaches?

The cyber security practices in the FDA and USDA guidance documents are very general in nature and address only the most basic cyber security practices. These recommendations are practiced by most IT departments within the sector, but may provide only rudimentary cyber systems protection. They are certainly not reflective of the cyber security protection levels needed to meet the current state of cyber risks. On the other hand, the practices and protocols contained in the more recent DHS published guidance documents represent cyber protection steps to meet the current state of cyber risk. Yet, few of these more advanced or sophisticated protective measures are found within the medium and small food and agriculture firms.

4. What, if any, are the limitations of using such approaches?

The guidance to the food and agriculture sector is so basic that it affords only minimal cyber risk reduction capability. However, DHS, NIST, and state level guidance provides the necessary level of sophisticated cyber risk management recommendations; the primary challenges to implementation are cultural, experiential, resources allocation and senior management focus issues within medium and small firms.

5. What, if any, modifications could make these approaches more useful?

Based upon NCFPD's assessment program, it appears that modification to the specific guidance is less a need than the construct of the national implementation framework (i.e. regulatory vs. guidance vs. cultural institutionalization) and the collaborative approach needed for successful broad sector adoption.

6. How do these approaches account for sector-specific needs?

Given the need for cross-sector and cross-firm cyber risk management, the current DHS and NIST guidance will meet the need. The implementation approach, however, must be customized for the sector. As indicated earlier in this response, implementing standards and framework for improving overall cyber security within the sector for adoption at the national level must be closely coordinated via extensive collaboration with industry organizations. Additionally, implementation must leverage the current food safety risk management culture to limit resistance within the sector and to ensure it becomes simply a component of food safety risk management with minimal regulatory aspects beyond the food safety focus. One recommended approach is to engage the industry organizations in collaboration with the sector's insurance industry and the financial community to institutionalize these standards and best practices as a part of their underwriting and rating functions.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

Based upon NCFPD assessments under the FASCAT program, successful deployment of proposed frameworks and best practices is only successful with sector specific effort that engages industry organizations, sector specific agencies within government, and key industry leadership. Additionally, the DHS hosted Food and Agriculture Sector Government Coordinating Council (composed of federal, state, tribal, territorial and local government representation) and the Industry Sector Coordinating Council should engage in any broad sector cyber risk management framework deployment effort. This was the model followed for the nation's food and agriculture defense effort.

8. What role can sector-specific agencies and related sector coordinating councils play in developing and promoting the use of these approaches?

As noted above. The GCCs and SCCs play a critical role in every significant sector defense effort since the promulgation of HSPD-9 in 2003. NCFPD is an active collaborator with these councils. The NCFPD FASCAT assessment program was developed and deployed in close collaborations with these councils. This model is essential for a successful creation of a new cyber risk reduction framework within the sector.

9. What other outreach efforts would be helpful?

Key industry leadership must be identified and engaged in the effort. This can be accomplished via industry organizations and via direct outreach to the leadership of firms that actively engaged with past sector defense efforts. Additionally, agriculture is the key economic engine for 44 states; governors, public health directors, and agriculture commissioners (and their national organizations) should be directly engaged in the implementation effort.

Specific Industry Practices

NCFPD reviewed current cyber risk reduction recommendations from key DHS and NIST guidance documents that best fit the food and agriculture sector. Based upon that review, feedback from the

sector, and the experience obtained through the FASCAT program, NCFPD offers the following for consideration in developing the framework and the cyber risk management practices:
Food and agriculture Sector asset owners and operators gained immediate benefits by adopting network-based cyber technologies to plan and manage their operations by extending the connectivity of their industrial control systems. Protecting a firm's networks and cyber based process control and information management systems is always, at some level, a question of balance and strict attentiveness on the part of IT professionals. On one hand, a system that is not connected to the Internet in any manner is more secure than one that is connected via firewalls and intrusions protection and detection systems. On the other hand, a network with no connection to the World Wide Web cannot benefit from the numerous advantages, capabilities and resources Internet connectivity can provide.

Connectivity does provide a pathway for increasingly sophisticated criminal activity. Vigilance and software maintenance are essential because Internet connectivity exposes network assets to cyber infiltration and subsequent manipulation of sensitive operations. Increasingly sophisticated cyber-attack tools can exploit vulnerabilities in commercial networks and inter-connected industrial control system components, telecommunication methods, and common operating systems found in modern industrial management and control systems. These basic steps are nearly always involved in any successful attack where the intent is to conduct some criminal activity inside of the targeted cyber system. For denial of services attacks, these steps are not necessary. An attacker who wishes to assume control of a control system is faced with three challenges:

1. Gain access to the control system LAN - Firewall(s), Internet Connections & Employee device connections
2. Through discovery, gain understanding of the process - Unprotected databases, systems or process documentation and diagrams and connected device or control point reference numbers
3. Gain control of the process - Authentication processes, Intrusion Systems, System or Process Control Databases

To gain access, the criminal may employ physical theft, break into a facility to steal access passwords, or connect an unauthorized link. They also may employ deception techniques, such as phishing, or masquerading as an IT contractor or technical support team member. Once inside the system, the criminal must explore it to find the information necessary to make a planned theft, disruption or seizure of system control possible. Finally, once access and sufficient system or network knowledge is gained, the intended criminal activity is initiated.
The information management systems that can be targeted in Food and agriculture organizations are varied, but fall into two main types. Examples are:

Information Systems:

Inventory management systems
Order/Buyer systems
Cash management systems
Employee recruiting systems
Human resources management systems
Invoice and payment systems
Sales management systems
Contract compliance management systems

Process Control Systems:

Electronic preventive controls
Automated failure detection controls
Contamination surveillance/detection systems
Process control systems
Automated quality control systems
Shipping and distribution systems
Transportation management systems
Digital security systems

To illustrate an attack directed to a food or beverage production operation, it is useful to consider a hypothetical scenario, based on actual cybercrime events targeted on other critical infrastructures. In the following brief scenario, the criminals seek to contaminate a product and with broad distribution to gain the maximum number of human casualties and to seriously damage the product producer. Furthermore, they intend to obfuscate the supply and distribution records databases so as to limit any effective product tracing and recall efforts.

Food & Agriculture Sector Cyber Risk Scenario Example

- Beverage firm with national distribution is targeted
- Insider threat results due to a corrupted recruiting & HR records systems
- A product is contaminated with a lethal agent by an insider
- Control systems and automated surveillance systems are compromised via malware introduced through unprotected laptop connection to the web
- Distribution control system is re-programed via malware access to ensure rapid, broad distribution of the contaminated product.

NCFPD Cyber Defense Recommendations for Firms in the Food and agriculture Sector:

When planning for cyber defense, it is useful to consider the Top Five Cyber Security Threats for 2012 recently summarized at the RSA Security Conference in San Francisco[2]:

1. Continuing attacks by idealistic young 'hactivists'.
2. The fact that 'Big Data' companies are taking control of users while profiting from user information.
3. Foreign governments have or will start to target “clouds” and similar types of digital businesses functions with advanced persistent threat (APT).
4. Attackers will make more use of mobile exploits for hacking into corporate networks.
5. Company employees, consultants, and business partners can always pose security risks.

The following suggests basic cyber defense steps to consider, and sources for more targeted solutions to meet any specific firm’s needs. All cyber protection strategies and solutions must be tailored to the needs of the individual business, but must also adhere to basic concepts for the optimum individual solution. Protecting an organization from these growing threats often is difficult and requires multiple layers of defenses, otherwise known as “defense in depth”. As every organization is different, this strategy should be based on a balance between protection, capability, cost, performance, and operational considerations. “Defense in depth” for most organizations should at least consider the following two areas:

1. Protecting the enclave boundaries; and
2. Protecting the computing environment.

Enclave Boundary

In protecting the nation’s physical borders, US Customs and Border Patrol (CBP), USDA, FDA and National Oceanic and Atmospheric Administration (NOAA) protect the country from dangerous imports.

[2] Jacqueline Emigh, NotebookReview.com Contributor | 3/6/2012

In the same manner, each sector firm must protect the boundaries of their networks, particularly where they connect to the World Wide Web. The enclave boundary is the point at which the organization's network interacts with the Internet. "Defense in depth" in the Enclave Boundary starts with:

1. Monitored Firewalls; and
2. Monitored Intrusion Detection Systems.

Computing Environment

It is also imperative that firm network systems and their components, whether process control systems, information databases or desk-top computers used by management and clerical staff, are each protected with up-to-date defensive software systems. Additionally, the operators must be trained on best network and computer-use practices; such uses need to be monitored for failures and lapses in adherence to these best practices. We are all human and we all make mistakes. The successful and protected organizations understand this and support, nurture, and work to sustain the training and professionalism of their employees. Defending computing hardware and software from attack may be the first line of defense against the malicious insider — or it may be the last line of defense against the outsider penetrating the enclave boundary defenses.

These defenses start with:

Authorized Local Network Devices
Operating System Patching/Updating
Operating System Hardening
Anti-Virus Updating
Change Control Process
Host-based Firewall
Vulnerability Scanning
Use Of Proxy Servers & Web Content Filters
Email Attachment Filtering
Monitor Logs

While the above recommendations are tailored to the food and agriculture sector, NCFPD responds to the more general NIST practices identified in the RFI as follows:

NIST recommended practices as they pertain to critical infrastructure components:

- *Separation of business from operational systems;*
- *Use of encryption and key management;*
- *Identification and authorization of users accessing systems;*
- *Asset identification and management;*
- *Monitoring and incident detection tools and capabilities;*
- *Incident handling policies and procedures;*
- *Mission/system resiliency practices;*
- *Security engineering practices;*
- *Privacy and civil liberties protection.*

1. Are these practices widely used throughout critical infrastructure and industry?

During its assessment processes, NCFPD found cyber risk reduction practices are employed within the sector but to varying degrees of sophistication and effectiveness. Large sector firms are more comprehensive in their cyber risk programs while medium and small firms have only the most basic practices in place.

2. How do these practices relate to existing international standards and practices?

For the large, international food and agriculture sector firms, international standards do play a role. However, for the medium and small firms, they seemingly have little relevance.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

Based upon NCFPD assessments, the NIST listed practices most relevant to the food and agriculture sector are (note however that this list is incomplete from the NCFPD perspective. See the above narrative for further explanation):

- Identification and authorization of users accessing systems;
- Asset identification and management;
- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures;
- Mission/system resiliency practices;
- Security engineering practices

4. Are some of these practices not applicable for business or mission needs within particular sectors?

NCFPD experience within the food and agriculture sector suggests the following NIST listed practices are of less significance to the sector due to its operational profile:

- *Separation of business from operational systems;*
- *Use of encryption and key management;*
- *Privacy and civil liberties protection.*

5. Which of these practices pose the most significant implementation challenge?

Based upon NCFPD assessment experience:

- *Monitoring and incident detection tools and capabilities;*
- *Incident handling policies and procedures;*
- *Mission/system resiliency practices.*

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

NCFPD found the SSA guidance is so basic they are implemented as a part of most IT system protective programs. The more sophisticated cyber risk reduction tasks are generally implemented based up event experience, or based upon recommendations of IT support contractors for most medium and small firms, as opposed to national standards and guidance for best practices.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

Given the burden of regulatory requirements for food safety and the narrow margins under which these firms generally operate, resource allocation to cyber risk reduction is and will continue to be a significant challenge necessitating substantial change in the operational culture of medium and small firms.

8. Do organizations have a formal escalation process to address cyber security risks that *suddenly increase in severity?*

It appears few, if any, medium and small firms within the food and agriculture sector have a methodology in place in advance of events; however, each firm reacts to events in an individual manner, normally dictated by the culture within the firm's management. Furthermore, regulatory response to a food safety event where IT systems may play a role significantly impacts the firm's response. Lacking a strong sector framework and established detailed sector guidance, the response is influenced by local management culture and the individual regulatory agency input to the firm.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

NCFPD assessments indicate the key concerns within the food and agriculture sector have less to do with individual privacy concerns and more to do with corporate intellectual property, proprietary transaction records, and proprietary process control information protection. However, it should also be noted that, for retail firms, affinity card information systems storing customer data are a concern. Significant effort is made to protect this information from security breaches.

10. What are the international implications of this framework on your global business or in policymaking in other countries?

NCFPD suggests broad international adoption of the proposed framework and cyber risk reduction practices, if appropriately tailored to the food and agriculture sector, could have significant positive impact on the safety of imported foods and the reduction of EMA events within the food supply chain. Framework adoption reduces supply chain costs and improves the efficiencies within these supply chains. It should also be noted, however, that regulatory burdens are a factor in the migration of some sector firms to overseas locations. Therefore, the deployment of any proposed cyber security framework for the food and agriculture sector must undergo a thorough cost-benefit analysis.

11. How should any risks to privacy and civil liberties be managed?

NCFPD recommends a balance between the need to protect the privacy of individual's information, that of partner firms, suppliers and customers across the supply chains (from farm to retail) and the need to protect the viability and safety of the nation's food system. As a result, the GCC, SCC, and industry organizations must engage in developing the sector-specific operational guidance and best practices proposed for the national cyber risk management framework.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the framework?

See the NCFPD recommendations listed at the start of this section.

Conclusion

NCFPD research suggests an un-nerving level of complacency regarding cyber risk reduction within medium and small firms. Most firms know if they are routinely targeted by cyber criminals generally, but may not be aware of a specific attack, particularly if they have not been attacked in the past. This is demonstrated by the Trustwave report cited at the beginning of this document. NCFPD recommends that all firms in the sector go to http://www.us-cert.gov for more information and resources. NCFPD is currently developing resources and tools to aid cyber risk assessment.

With the globalization of our food system, both unintentional food safety threats and intentional adulteration or attacks on the food system are common occurrences. Defending the food and agriculture sector against increasingly dangerous and challenging cyber threats is imperative to protecting stakeholders from serious financial, reputational, and health consequences

POCs for this document are:

John T. Hoffman
Colonel, USA Retired
Senior Research Fellow
Hoffm584@umn.edu

Andrew Huff, MSST
Research Fellow
Ph.D. Candidate
National Center for Food Protection and Defense University of Minnesota
andrewgeorgehuff@gmail.com

National Center for Food protection and Defense
University of Minnesota
A US Department of Homeland Security Center of Excellence
120 LES Bldg.
1954 Buford Ave.
St. Paul, MN 55108
Office: 612-626-6359