

**CRITICAL INFRASTRUCTURE AREAS IN  
AGRICULTURE AND FOOD  
IN THE UNITED STATES**

September 27, 2007

## **Critical Infrastructure areas in Agriculture and Food in the United States**

### **Abstract**

The protection of critical infrastructure areas related to agriculture, food, and homeland security becomes the issue of the day. Critical infrastructures embrace a wide range of highly complex and multinational collections of processes, technologies, and people, thus being vulnerable to potential failures. The present research discusses critical Infrastructure areas in Agriculture and Food and Homeland Security in the U.S, examines approaches to modeling critical infrastructures, analyses strategic plans and initiatives developed by the U.S. government in order to enhance recognition of new technologies for the homeland security, and agriculture and food areas. The research also discusses the roles and responsibilities for the critical infrastructure protection, adequacy and status of the efforts on different levels (including federal efforts to fulfill the responsibilities involved), as well as the challenges faced in critical infrastructure areas related to agriculture, food, and homeland security. Finally, the present study is based on the experience of the most reliable coordination centers and information sources thus providing the most comprehensive and detailed overview of the critical infrastructure areas related to agriculture, food, and homeland security.

**Critical Infrastructure Areas in Agriculture and Food in the United States**

Table of Contents

1. Introduction
2. Critical Infrastructure areas in the United States
  - A) Critical Infrastructure: Areas of National Economy and Industry
  - B) National Strategies
  - C) The Retaliation Systems
  - D) Planning and Accomplishment of Appropriate Organizational and Technical Measures
3. Conclusion

## **Critical Infrastructure areas in Agriculture and Food in the United States**

### Introduction

The expenditures for industrial, exploratory, and producing systems are measured in millions and billions dollars; no wonder that the issues related to homeland security, defense and protection become the issues of primary importance. Their importance increases along with the dependence of these sectors and areas from critical infrastructure of the country. Forming of opinions and priorities in the areas related to Agriculture and Food, and Homeland Security can be examined by the example of the United States, in the capacity of the country, which is to a greater or lesser extent is subjected to the threat of terrorism (Hohlstein, 2002).

The U.S. government undertook a complex of measures aimed to protect its critical infrastructure. For example, in 1997 the presidential commission performed a report dedicated to protection of critical infrastructure in the United States (Chalk, Hitting America's Soft Underbelly, 2004). This report became an initial point for the beginning of large-scale measures, which were undertaken by the U.S. government in order to enhance the level of protection of the U.S. critical infrastructure.

In 1998 the U.S. President approved the decree no.63 (PDD63), according to which critical infrastructure was defined as physical and information systems that are necessary and strategically important for maintenance of minimum acceptable level of functioning of economy and government. In accordance with the PDD no. 63 critical infrastructure basically includes telecommunications, transportation, water supply systems, and emergency services, to mention a few. From here it follow that critical infrastructures embrace a wide range of highly complex and multinational collections of processes, technologies, and people, thus being vulnerable to

potential failures. No wonder that protection of critical infrastructure areas related to agriculture, food, and homeland security becomes the issue of prime importance for the United States.

### Critical Infrastructure Areas in the United States

#### Critical Infrastructure: Areas of National Economy and Industry

As it was already mentioned before, the critical infrastructure in the United States embrace such important areas of national economy and industry like national defense, agriculture (about 2 million farms), food industry (about 87,000 plants and factories), civil aviation (5,000 airports), marine transport (300 ports), 590,000 highways and bridges, 400 tunnels, 80,000 dams, 2,000,000 miles of pipeline, water supply (3,400 reservoirs), health care sector (5,800 hospitals), emergency services (87,000 brigades), state run public authorities (3,000), military designation industry (250,000 companies), information and telecommunication systems and networks (2 billion miles of cable), power engineering (2,800 electric power stations), 104 atomic power stations, transport, banking and finance systems (26,600 departments), chemical industry (66,000 plants), postal services (137 million mailboxes), 460 tower buildings, and 5,800 national and historical sites (Annual Energy Outlook 2007. DOE/EIA-0383 (2007)).

It should be taken into consideration that 85 percent of critical infrastructure in the United States is a private property of entrepreneurs (small-, mid- and large-size business companies), who use infrastructure for production of commodity and services (Challenges for Critical Infrastructure Protection GAO-03-233, 2003). From here it follows all the complexity and importance of the issues related to protection of critical infrastructure, especially concerning Food and Agriculture in the United States.

#### National Strategies

In compliance with the PDD no.63, the main components of governmental strategy related to the areas of defense of critical infrastructure are as follows:

- The importance of cooperation and collaborative work between public and private sectors in the United States (Council, 2002);
- Head federal agencies responsible for every critical infrastructure area;
- Coordination groups and work groups aimed to coordinate the efforts of federal agencies and industrial groups (Katz, 2005);
- Information exchange systems for every sector of industry, referred to as ISACs – Information Sharing and Analysis Centers (Maguire, 2003);
- The necessity to create safety plans aimed to provide safety for national infrastructure. These plans will develop and maintain control issues to analyze vulnerabilities and to prepare efficient plans for elimination of all possible vulnerabilities in every area of industry;

In 2001 (soon after the events of September 11) the U.S. government approved the act, under which the plan of protection of critical infrastructures in the U.S. was developed (USA Patriot Act of 2001, October 2, 2001). In 2002 the government approved Homeland Security Act. In compliance with the act there was created DHS (Department of Homeland Security), and the post of director responsible for analysis of information and infrastructure protection was approved. In 2003 the U.S. president upheld a decision to develop national strategy related to maintenance of cyberspace safety. This document was addressed to American society and was aimed to enhance and widen cooperation and consolidation of efforts of the U.S. citizens, federal, state, government, non-government, and private organizations in order to develop an efficient strategy to withstand cyber terrorism.

#### The Retaliation Systems

The major part of the strategy sets priorities aimed to facilitate the development of retaliation systems, the programs aimed to withstand threats and vulnerabilities, educational programs, programs aimed to enhance the level of awareness, national and international cooperation, to mention a few. Further the complex of measures aimed to enhance the level of national protection of industrial systems (especially related to protection of critical infrastructure areas related to agriculture, food, and homeland security) were proclaimed a national priority. These measures include HAACCP regulation (Food safety Hazard Analysis and Critical Control Point Regulation), GRAS (Generally Recognized As Safe) determinations (Orszag, 2003), various food and nutrition support initiatives, product labeling, pathogen detection, product recall and product rebranding, plant and animal health, international trade regulations and guidelines (i.e. phytosanitary and sanitary inspections, import-export issues, etc), economic regulation (Prah, 2005), Homeland Security for the agriculture and food sector, agricultural research, and intellectual property law, to mention a few (National Agricultural Statistics Service (NASS), 5). The vast majority of these issues are encompassed in the Environmental Protection Agency, the Food and Drug Administration, the USDA portfolio, the Department of State and the Office of the U.S. Trade Representative, the Department of Commerce, the Federal Trade Commission, the Department of Health and Human Services, the U.S. Department of Justice, and the Department of Transportation, in all issues related to critical infrastructure protection, antitrust law enforcement and food advertising (The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, 2003).

Since that time the measures aimed to enhance the level of national protection of industrial systems involve participation of the developers, owners of these systems, along with consultants, scientific and research organizations, independent associations, and federal

authorities, to mention a few. In order to develop technical and technological solutions for protection of industrial systems in critical infrastructure areas related to agriculture, food there were created numerous laboratories in research centers, such as National SCADA Test Bed, and many others. In result of these collaborative actions, there were developed many standards and guides related to various aspects of maintenance of the industrial systems security (Jordan 12).

For example, Digital Bond Inc. created control center protection profile for industrial control systems. Under this profile the company developed a list comprising of 22 kinds of potential threats and vulnerabilities related to the industrial control systems. On the ground of the given list of threats and vulnerabilities there were formulated 28 strategic tasks of protection comprising of 55 components of functional safety requirements and 17 components of secured and warranted estimation in compliance with the general criteria defined under the given control center protection profile (Personal communication and non-public data, 2005). This company also developed the set of signatures of network attacks for Modbus TCP and DNP3 protocols used in industrial systems. These signatures were initially developed for Snort system within the frameworks of research project financed by the National Security Department. Symantec and ISS, the leaders in information security market, also added support for these signatures into their corresponding products. Cisco modified these network attack signatures for use in its platforms (S198 Signature Update for Cisco IDS 4.1 and IPS 5.0). The scientists and researchers continue to develop the efficient mechanisms of protection for other network protocols used in industrial systems (also in Agriculture and Food Industry).

#### Planning and Accomplishment of Appropriate Organizational and Technical Measures

During the course of planning and accomplishment of required organizational and technical measures for protection of industrial systems in Agriculture and Food areas the

developers conduct their activities in compliance with the international IB standards (namely, ISO/IEC 17799:2005). According to them, control mechanisms are applicable to industrial systems. Taking into consideration the advanced requirements for protection of critical infrastructure, especially in relation to Agriculture and Food and Homeland Security areas in the United States, it is recommended to use additional special purpose standards and guidelines developed in the course of large-scale measures for protection of critical infrastructure (Chalk, *The Bio-Terrorist*, 2003). These special guidelines are very important, because the previous recommendations and standards predominantly include basic safety mechanisms, which are not very efficient. These special guidelines include “Urgent Action Standard 1200 — Cyber Security”, and *Cryptographic Protection of SCADA Communications, Part 1: Background, Policies, and Test Plan*”, to mention a few.

Protection of industrial systems related to critical infrastructure in the United States (especially what concerns Agriculture and Food areas) from cyber terrorism gradually becomes the issue of primary importance in homeland security areas. This issue becomes extremely important, when the increased level of terrorism threat is combined with the incredibly increasing level of dependence of the civil society from industrial systems (Federal Policies for Infrastructure Management, 1986). Therefore, it requires coordinated and all-embracing complex of efficient measures both from the government and from industrial sector of the country. Although there are no significant terrorist attacks at the moment, the threat still can be expected.

### Conclusion

In conclusion it may be said that the vast majority of industrial systems used in Food and Agriculture areas in the United States have vulnerabilities similar to those of other IT systems. Yet, there are vulnerabilities specific for these areas of critical infrastructure. In order to

provide adequate and corresponding protection of the system employed in Agriculture and Food areas, the developers should undertake significant efforts in order to enhance the level of protection for their products, along with developing additional build-in safety functions in compliance with the requirements of specific security profiles with subsequent certification of these products. The owners and organizations that use industrial systems related to Agriculture and Food areas should change and thoroughly reexamine their attitude towards information security issues along with the existing system of priorities currently in force.

The important role in making decisions concerning the security issues of industrial systems of critical infrastructure related to the Agriculture and Food areas should play the U.S. government, national security authorities, and anti-terrorism structures. In addition, it should be also taken into consideration that in order to develop and conduct corresponding scientific and research projects, to develop appropriate and efficient standards, methodology, protection frames and protection mechanisms for industrial systems the developers will require significant state financing, large-scale national programs and legal regulation.

## References

- (2007). *Annual Energy Outlook 2007*. DOE/EIA-0383 (2007). Energy Information Administration.
- Chalk, P. (2004). *Hitting America's Soft Underbelly: The Potential Threat of Deliberate Biological Attacks Against the U.S. Agricultural and Food Industry*. Santa Monica, CA: RAND.
- Chalk, P. (2003). *The Bio-Terrorist Threat to Agricultural Livestock and Produce*. Testimony before the Senate Government Affairs Committee.
- (2003). *Challenges for Critical Infrastructure Protection GAO-03-233*. General Accounting Office (GAO).
- Council, N. R. (2002). *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Academies Press.
- (1986). *Federal Policies for Infrastructure Management*. Congressional Budget Office (CBO).
- Hohlstein, R. (2002). *Food Fight: the Battle to Protect our Food and Water against Terrorism*. Madison, WI: Goblin Fern Press.
- Jordan, M. *CRS Report RL31734, Federal Disaster Recovery Programs: Brief Summaries*.
- Katz, L. (2005). *Agroterrorism: Another Domino*. New York: Novinka Books.
- Maguire, S. (2003). *CRS Report RL33770, Department of Homeland Security Grants to State and Local Governments: FY2003 to FY2006*. Department of Homeland Security.
- (5). *National Agricultural Statistics Service (NASS)*. U.S. Department of Agriculture.
- Orszag, P. (2003). *Homeland Security and the Private Sector*. The Brookings Institution.
- (2005). *Personal communication and non-public data*. U.S. Postal Service.
- Prah, P. (2005). Is the U.S. Ready for Another Major Disaster? *CQ Researcher*, 15 (21).
- (2003). *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*. Office of the President.