Synopses of
"The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets"
The White House February, 2003

This February 2003 White House report is the basis for reorganizing Federal Homeland Security activities and identifies the infrastructure protection objectives of the new Department of Homeland Security. The report details eleven (11) infrastructure sectors and five (5) key asset categories of concern the Federal government has identified as being critical to achieving U.S. Homeland Security objectives.

A. Cross-Sector Security Priorities

The common issues that cross-cut multiple parts of the infrastructure are identified as Cross-Sector Security Priorities.

1. Planning and Resource Allocation is risk assessment and protection planning for critical parts of the infrastructure.

2. Information Sharing and Warnings is networking threats and threat indicators to get appropriate warnings out.

3. Personnel Security, and Building Human Capital and Awareness addresses screening and monitoring personnel to avoid adverse actions by insiders, and building a trusted, capable core of employees in charge of critical infrastructure. It also seeks to raise awareness of national security issues to individuals.

4. Technology, Research and Development is focused on the need for more sophisticated surveillance and detection technology.

5. Model Simulation and Analysis is concerned with infrastructure risks, the potential of impairments, the impacts of those impairments, and the alternatives that are available should part of the infrastructure become unavailable.

B. Securing Critical Infrastructure and Key Assets

The report identifies the critical infrastructure and key asset protection issues as follows:

1. Agriculture and Food Sector includes the supply chains for animal feed and animal products, and crop production including the supply chains for seed, fertilizer, and other materials. It also includes post-harvesting components such as processing, production, packaging, storage, and distribution. Distribution includes retail, institutional, restaurant, and home consumption. A major component is prevention and detection of contamination. Vulnerabilities include the farms themselves, food processing plants, and the distribution chains including transportation, food stores, and restaurants. Critical issues are the response to prevention and detection of contamination, identifying distribution risks, and containing risks once they are identified.

2. Water includes physical damage, destruction, or contamination of water supplies and wastewater treatment facilities. This can be in the form of loss of controls, or sabotage of information management systems that control water treatment, or infrastructure disruption,

including pipelines, tankage, and pumping stations. Vulnerabilities are the supply sources, reservoirs, aquifers, etc. The need to establish monitoring and analysis capabilities is identified as are the need for plans for emergency response should a threat or actual contamination occur. It also establishes awareness of water's interdependence with other critical industries and activities.

3. Public Health has as its primary issue: contamination. Exposure of the public or emergency responders can lead to contamination of the public health infrastructure, or it could be directly targeted or compromised by mishandling of patients. Vulnerabilities include security of health care facilities, pharmaceutical supplies, and protection of medical staff. On a larger scale, dealing with public health epidemics and isolation of parts of the general population must be addressed. The challenges include communication and planning to handle large numbers of contaminated or ill people, isolating them and protecting the facilities and health care workers from contamination. Protecting and decentralizing medical and drug supplies is also key.

4. Emergency Services includes fire, rescue, emergency medical, and law enforcement organizations and their people responding to CBR (chemical, biological, radiological) agents. Initiatives already identified are: interoperability of communication systems, redundancy of communication networks, protection of facilities and equipment associated with emergency response, protection of emergency responders, training exercises and planning, mutual aid among local jurisdictions, and capability to link up with appropriate Federal resources.

5. Defense Industrial Base includes security of military bases and military contractors at all levels. Key issues are security of the physical property and surety of the Federal and private employees in these facilities. Concerns relate to military installation operation, maintenance, manufacturing of critical military goods, storage and transport of military goods, and security of the industry base that provides these goods.

6. Telecommunications includes all public and private communication assets, including the public network infrastructure, the internet, and private enterprise networks. Physically these are the telecommunication centers, transmission towers, relay towers, fiber optic cables, antennae, and other communication equipment that form the telecommunication infrastructure for voice and data. The priority here is service reliability and security. Concerns to be addressed are the vulnerability of facilities and transmission equipment, personnel surety, and capability for alternate telecommunication routing through the existing telecommunication architecture.

7. Energy concerns are associated with the continuity of production of electric power, which affects all sectors of the economy and nearly all of the infrastructure. The concerns here are loss of power plants, substations, transmission lines, or interruption of fuel supply. Vulnerabilities needing to be addressed include: physical plant and transmission security, stockpiling of critical components, and evaluation of system restoration and recovery after attack. A subset of the concerns are the fuel transportation distribution network vulnerably which includes: ports and terminals, pipelines, refineries, processing plants, and storage and pumping stations much of which are addressed under Transportation. Physical security and personnel surety are a large component of the energy security. Restoration after attacks and alternate energy supply capability are part of recovery concerns. Nuclear energy is identified separately in the "Protection of Key Assets" category.

8. Transportation includes aviation, rail, highway, trucking, pipelines, and maritime operations. Physical plant and component security is paramount for airports, rail stations, marine ports, fuel depots, transportation depots, storage facilities, maintenance and repair facilities, bridges and tunnels. In addition, modes of transportation could be used as attack delivery mechanisms. Personnel surety and detection of contraband is a critical component of this infrastructure sector. In some transportation modes, screening of both passengers and freight is required. Intermodal transportation centers are also important, especially containership terminals, and intermodal train and truck terminals. Alternate routing and substitution transportation modes are backup considerations. All these transportation systems depend on secure fuel supplies, depots, and availability of prime movers. Fuel pipelines and pumping stations are also in this category. Physical security of facilities and surety of key staff are part of security concerns. Light rail mass transit systems, passenger trains, commercial airliners, and buses are considered primary targets and are vulnerable places where the public should be protected.

9. Banking and Finance concerns revolve around physical infrastructure and business transactional capability. Much of this ties back to security of electronic networks and telecommunication services. Backup files and systems and surety of personnel are also key.

10. Chemical Industry and Hazardous Materials are also cross-tied to agriculture, water supplies, and energy. Chemicals and manufactured material, impact other parts of the infrastructure. The concern here is protection of physical plant and personnel surety. Chemical plants that are critical to the defense infrastructure and other infrastructures need to be identified. Control of unwanted distribution or misuse of hazardous chemicals as weapons is a factor. This is especially true for highly toxic substances, such as pesticides, and explosives, or components of explosives, such as some fertilizers.

11. Postal and shipping concerns include handling the mail and parcels. Much of it is related to continuity of business. It includes the U.S. Postal Service and other package handlers. These networks are vulnerable at points of entry for parcels and letters. Parcels and letters that are moved through the transportation network, including airplanes, trains, and highway vehicles are also a concern. Screening and detection of contraband in letters and packages is a vulnerability. Proper customer identification, screening and detection techniques, and surety and protection of postal and shipping personnel are concerns.

12. Protection of Key Assets including icons, landmarks, historical buildings and attractions, centers of government, technology and commerce are a concern. The subcategories under Key Assets are as follows:

    a. National Monuments and Icons are to be physically protected and the visitors to them also protected. Challenges and vulnerabilities are site security, screening of visitors, surety of the staff, contractors and other workers and suppliers, and the risks of high profile incidents at these highly recognizable venues.

    b. Nuclear Power Plants are identified separately from the rest of Energy infrastructure. They are among the more secure parts of the private sector infrastructure today, but also attractive targets. Concerns address raising the level of physical security and protection regarding the surety of employees, contractors, suppliers, and others that live near, or have access to, these sites and facilities.

c. Dams are often linked to water resources and energy and tied to regional population centers and agriculture. They are identified separately as they are uniquely attractive targets. Physical protection of dams from sabotage involves physical protection of the site, access to the site, and surety of the employees, visitors, contractors, and other suppliers.

d. Government Facilities represent high profile Federal buildings. Employee and contractor access to these facilities is a vulnerability. In addition, in many Federal buildings there are non-Federal tenants, business visitors, and even tourists. Physical security and surety of contractors, employees, and visitors is key.

e. Commercial Key Assets include business and commercial properties that conduct transactions, and perform business functions. Some of the tenants of commercial buildings may be high profile organizations which could be targets. In other cases, the buildings themselves may be well-known icons, which would make them attractive targets. Issues include building security, and screening of employees, contractors and visitors.