Chapter 7: Critical Infrastructure Protection

Mission

The Bureau of Industry and Security (BIS) – through its Critical Infrastructure Assurance Office (CIAO) – coordinates private sector input into the national strategies for cyber security and homeland security, and leads the Federal Government's outreach efforts to industry on critical infrastructure protection and cyber security issues.

Under Secretary Kenneth I. Juster addresses the Commerce Department's Patriot Day Ceremony, September 11, 2002.

The CIAO supports activities that protect the following identified critical infrastructure sectors: agriculture, food, water supply, public health, emergency services, government services, defense industrial base, information and telecommunications, energy, banking and finance, transportation, the chemical industry, and postal and shipping. These industrial sectors are deemed "critical" because their incapacity or destruction could have a debilitating regional or national impact on our quality of life. The Federal Government is concerned with the readiness, reliability, and continuity of key services within these sectors – both physical and cyber.

Accomplishments in Fiscal Year 2002

Public Private Partnerships

Acting alone, the Federal Government cannot hope to secure our nation's critical infrastructures. Infrastructure assurance can only be achieved by a voluntary public-private partnership of unprecedented scope, involving business and government at the Federal, state, and local levels. Forging a broad-based partnership between industry and government lies at the heart of the CIAO's mission.

The CIAO seeks to engender awareness among the owners and operators of the nation's critical infrastructures (both private sector and state and local government) on the need to secure their assets, systems, and networks against deliberate physical and cyber attacks. As described in Chapter 4 of this report, the CIAO organizes and participates in local, regional, and nationwide conferences and events presenting and educating the public and private sector on critical infrastructure protection issues.

Partnership for Critical Infrastructure Security

The CIAO supports the Partnership for Critical Infrastructure Security (PCIS), an organization that provides a unique forum for government and private sector owners and operators of critical infrastructures to address and discuss common issues and share information across industry sectors. The mission of PCIS is to identify and

address infrastructure security matters common to all sectors because of increased reliance on shared information systems and networks.

Representatives of more than 70 Fortune 500 companies involved in critical infrastructure industries are members of PCIS. Through participation in workshops and forums, such as the "Annual Cross Sector Information Sharing Meeting," and "Keep America Working: Securing Digital Control Systems for the Nation's Critical Infrastructures," the CIAO supported PCIS efforts to educate members and facilitate cross-sector cooperation and problem solving.

National Infrastructure Advisory Council

The CIAO was tasked with providing staff support for the National Infrastructure Advisory Council (NIAC), an advisory committee composed of up to 30 private sector representatives to provide counsel to the President on national critical infrastructure assurance issues. The NIAC will provide advice and make recommendations on enhancing cooperation between the public and private sectors in protecting information systems supporting critical infrastructures, proposing and developing ways to encourage private industry to perform periodic risk assessments of critical information and telecommunications systems, and monitoring the development of private sector Information Sharing and Analysis Centers (ISACs) as well as providing recommendations on how these organizations can best foster improved coordination among the ISACs and between the ISACs and the government. The NIAC will begin its work in Fiscal Year 2003.

Digital Control Systems Conferences

In February 2002, the CIAO coordinated a meeting, hosted by the Chairman of the President's Critical Infrastructure Protection Board, consisting of government leaders, technical experts, and appropriate policy and regulatory staff to discuss security shortcomings in existing digital control systems, ways to improve security, and the government's role in improving security. Digital control systems are a category of computer and networked systems that manage the delivery of key industrial services including electricity, water, and transportation.

In April 2002, the CIAO and PCIS convened a meeting with owners and operators of facilities in various critical infrastructure sectors, government representatives, and digital control system vendors. The purpose of the meeting was to lay out the scope of dependency on digital control systems, the landscape of the obstacles to securing such systems, and a list of potential high-return initiatives to address them. PCIS has agreed to take the lead in this initiative because it has the unique ability to engage various sectors in cross-sectoral issues.

Information Sharing and Analysis Centers

One of the most important methods of managing the security of critical infrastructures is intra-sector and cross-sector coordination and information sharing. Information Sharing and Analysis Centers (ISACs) are a mechanism to share information about vulnerabilities, threats, and incidents, and to analyze the information for common trends within a sector or among different sectors.

Since the events of September 11, the CIAO has helped facilitate the creation of ISACs in many of the newly-identified critical infrastructure sectors, including in the healthcare, insurance, and chemical sectors. The CIAO continues to support mature ISACs in identifying emerging needs and in working strategically with all of the ISACs.

In conjunction with the White House Office of Cyberspace Security, the CIAO coordinated the second annual meeting of ISACs in Fiscal Year 2002. The objectives of the meeting were to update the ISACs on the current status of ISAC formulation in certain key infrastructure sectors, share information across critical infrastructure sectors, and plan next steps. The CIAO provided support, facilitated discussion, and convened members of these groups to ensure communication and cooperation between and among ISACs.

International Activities

BIS's involvement in critical infrastructure assurance issues has extended beyond the borders of the United States. The CIAO participated in the U.S.-India Cyber Terrorism Initiative on March 26, 2002, and CIAO representatives attended both the U.S.-India and the U.S.-Italy Bilateral Critical Infrastructure Protection Sessions on May 2-3,

2002 in Rome, Italy. The CIAO continues to support other U.S. critical infrastructure protection-focused bilateral meetings.

In addition, the CIAO has an ongoing partnership with Canada's Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). The CIAO delivered several briefings on the topic of building public-private partnerships to staff from agencies across the Canadian Government in October 2002. In addition to the CIAO's briefings for OCIPEP officials, the Associate Deputy Minister of OCIPEP has participated in several of the CIAO's outreach activities in the United States, such as the CIAO-CXO Media Policy Forums described in Chapter 4.

Secretary of Commerce Donald L. Evans addresses the Homeland Security Tech Expo, September 19, 2002.

Cyber Security Education

The CIAO has worked with the National Education and Training Program for Infrastructure and Information Assurance to increase the number of information technology professionals who protect our computer networks and the information stored in them, cyber infrastructures, and management information systems by increasing the number of people studying this issue.

State and Local Critical Infrastructure Protection

The CIAO – in partnership with senior state officials – sponsored and managed two successful state conferences that addressed lessons learned from September 11, including lessons learned in the areas of homeland security and critical infrastructure protection. The focus of the conferences was to improve cooperation between private industry and local, state, and Federal governments to address the challenge of ensuring the protection of essential services in the event of a terrorist attack or significant breach of security.

The conferences were held on February 12-13, 2002 in Austin, Texas and on April 23-24, 2002 in Princeton, New Jersey. The state conference series has been instrumental in assisting the CIAO towards completion of *Effective Practices on Critical Infrastructure Assurance*, a tool that communities can use to assure their own critical infrastructures. The compendium of *Effective Critical Infrastructure Assurance Practices*, resulting from the Effective Practices Working Groups identified in the CIAO's state conferences, and the establishment of a consortium of academia, government and private sector partners, will aid communities across the United States.

Federal Government Policy and Initiatives

President's Critical Infrastructure Protection Board

By signing Executive Order 13231, the President created the President's Critical Infrastructure Protection Board and gave it responsibility for "ensur[ing] protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems." BIS has been instrumental in supporting the work of the Board. The Under Secretary for Industry and Security and the Director of the CIAO both are Board members. The Under Secretary also chairs the Committee on Private Sector and State and Local Government Outreach, which, among other things, is responsible for coordinating outreach to and consultation with the private sector, including corporations that own, operate, develop, and equip information, telecommunications, transportation, energy, water, health care, and financial services on protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. The Committee also is responsible for coordinating outreach to state and local governments, as well as communities and representatives from academia and other relevant elements of society.

National Strategies for Homeland Security and Cyberspace Security

A national strategy provides a foundation and a common framework for roles, responsibilities, and concerted action. It also helps to establish, with the Congress and the American public, the basis for proposing legislative and public policy reforms where such reforms are needed to advance national policy.

To address the need to defend against the threat of physical attack upon our nation's homeland, President Bush established the Office of Homeland Security (OHS). On July 16, 2002, the President issued the *National Strategy for Homeland Security*, an overarching strategy for securing the American homeland. This overarching strategy is being further detailed in two components, which include:

- the *National Strategy to Secure Cyberspace*, focusing on protecting information systems and networks; and
- the *National Strategy for the Physical Protection of Critical Infrastructures and Key Asset*s, providing specific implementation strategies, including roles and responsibilities.

In conjunction with the staff of the President's Critical Infrastructure Protection Board, the CIAO participated in the development and drafting of the *National Strategy to Secure Cyberspace*, including facilitating and coordinating the efforts of the Lead Agency Sector Liaison officials and sector representatives concerning the preparation by the private sector of input for the strategy.

OHS also enlisted the CIAO's help in developing the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, which will aid in the protection of the physical facilities of critical infrastructure systems. In addition to helping OHS with the national physical and cyber security strategies, the CIAO provided both facilitation and analytical support for a series of workshops on physical critical infrastructure protection with industry and state and local governments.

Federal Asset Dependency Analysis

The CIAO is responsible for assisting civilian Federal agencies with analyzing their dependencies on critical infrastructures to ensure that the Federal Government is able to continue to deliver services essential to the security, economy, and health and safety of its citizens, despite deliberate attempts by a variety of threats to disrupt such services through cyber or physical attacks.

To carry out this mission, the CIAO developed Project Matrix,™ a program designed to accurately identify and characterize the assets and associated infrastructure dependencies and interdependencies the Federal Government requires to fulfill its most critical responsibilities to the nation.

Project Matrix™ involves a two-step process in which each civilian Federal agency identifies critical assets (Step 1) and identifies other Federal Government assets, systems, and networks on which those critical assets depend to operate, as well as all associated dependencies on privately-owned and operated critical infrastructures (Step 2). Because of constant changes in the agencies' infrastructures, a continuing information "refreshment" step is needed to keep the Matrix database accurate and reliable.

In Fiscal Year 2002, 17 Federal agencies had entered the Matrix process, with three agencies having completed Step 1 and two agencies having completed Step 2. Currently, six agencies are in the process of completing Step 1. The Matrix analytical work for Step 2 for four additional agencies has been completed, and the Matrix team is in the process of preparing a report on each agency.

Goals for Fiscal Year 2003

BIS will continue to develop partnerships at the senior executive level with industry, as well as state and local government, to address governance, core management practices, and risk-based investment decision-making criteria in the area of critical infrastructure protection. Specifically, the CIAO plans to help secure digital control systems through the PCIS, announce and convene meetings of the NIAC, and develop the new health care, insurance, and chemical ISACs while supporting the existing ISACs.

The CIAO also will continue its series of state conferences and compile *Effective Critical Infrastructure Assurance Practices* to aid local communities. Finally, the CIAO will continue to initiate Project Matrix Steps 1, 2, and refreshment steps, and coordinate the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* for external review in Fiscal Year 2003.

In accordance with the Department of Homeland Security Act of 2002, it is anticipated that the CIAO will move to the Department of Homeland Security by March 1, 2003, and will cease to be a part of BIS.