Return to Table of Contents

Chapter 8. Critical Infrastructure Assurance Office

The Critical Infrastructure Assurance Office (the CIAO) is an inter-agency office located within the Bureau of Export Administration.

The CIAO was created as a mechanism to assist in the coordination of the U.S. Government's initiatives on critical infrastructure protection. Critical infrastructures comprise those industries, institutions, and distribution networks and systems that provide a continual flow of goods and services essential to the nation's defense and economic security and the health, welfare, and safety of its citizens. These infrastructures are deemed "critical" because their incapacity or destruction could have a debilitating regional or national impact.[1]

The CIAO's responsibilities include:

- coordinating the development of an integrated national strategy for critical infrastructure protection;
- coordinating departmental analyses on how to lessen unacceptable risks resulting from the U.S. Government's dependencies on critical infrastructures;
- coordinating national education and awareness programs targeted toward increasing public understanding and participation in protection efforts; and
- coordinating legislative and public affairs to integrate infrastructure assurance objectives into the public and private sectors.

In carrying out its mission, the CIAO has focused on critical infrastructure issues that cut across industry sectors and are not the responsibility of existing departments and agencies, thereby ensuring a coherent and cohesive federal approach to national critical infrastructure assurance.

Executive Order 13231: Critical Infrastructure Protection

In May 2001, the Bush Administration announced that it would be developing a national strategy for critical infrastructure protection and that the CIAO would coordinate the development and preparation of the strategy.

---

[1] These infrastructures relate to: information and communications; electric power generation, transmission, and distribution; oil and gas storage and distribution; banking and finance; transportation; water supply; and emergency assistance.

On October 16, 2001, President Bush signed Executive Order 13231, *Critical Infrastructure Protection in the Information* Age (the Order). The Order sets forth the policy of the United States to protect against disruption of information systems supporting the nation's critical infrastructures. The Order establishes the President's Critical Infrastructure Protection Board (the Board) to coordinate federal efforts and programs that relate to information systems supporting the nation's critical infrastructure and involve the following:

- cooperation with and protection of private sector infrastructures, state and local governments' critical infrastructures, and supporting programs in corporate and academic organizations;
- protection of federal departments and agencies critical assets and information systems; and
- related national security programs.

The Board coordinates its activities with the White House's Office of Homeland Security and the National Security Council.

The Special Advisor to the President for Cyberspace Security chairs the Board. The Board is made up of Cabinet-level and other senior government officials. The Order assigns a number of key responsibilities to the Department of Commerce and the CIAO, primarily in the area of national outreach and awareness. The Department of Commerce has two Board members: the Under Secretary for Export Administration serves as the designee of the Secretary of Commerce, and the Director of the CIAO also is designated as a member of the Board. The Under Secretary for Export Administration also chairs the Board's standing committee on Private Sector and State and Local Government Outreach.

FY 2001 Activities

During FY 2001, the CIAO's responsibilities in developing and coordinating national critical infrastructure policy focused on four key areas:

- promoting national outreach and awareness campaigns in the private sector;
- assisting federal agency analysis of critical infrastructure dependencies (e.g., Project Matrix);
- coordinating national awareness and outreach programs; and
- coordinating the preparation of an integrated national strategy for critical infrastructure assurance.

Promoting National Awareness

The CIAO worked with the private sector and other federal agencies to raise awareness of the importance of critical infrastructure protection. The primary foci of these continuing efforts are the owners and operators of critical infrastructures (i.e., information and communications, electric power, oil and gas, banking and finance, transportation, water, and emergency responders and critical government services). In addition to infrastructure owners and operators, awareness efforts have also targeted other influential stakeholders in the economy. The CIAO promoted activities that inform business and technology leaders across a variety of industry sectors of the need to manage the new risks associated with increased reliance on electronic information systems. The target audiences for these activities are the mainstream business, risk management, legal, financial analysis, and state and local government communities. In addition, the CIAO began a program of "in-reach" within the Department of Commerce to explore and take advantage of existing relationships that other entities in the Department already have with the private sector.

The CIAO focuses on initiatives that cut across industry sectors and are not the existing responsibility of other U.S. Government agencies. Three of the CIAO's major outreach and awareness initiatives during FY 2001 were:

- the Partnership for Critical Infrastructure Security;
- outreach to the business community; and
- support for federal lead agencies.

Partnership for Critical Infrastructure Security

As individual federal agencies formed partnerships with each critical infrastructure sector, a need emerged for cross-industry dialogue and sharing of experience to improve the effectiveness and efficiency of individual sector efforts. The Partnership for Critical Infrastructure Security (PCIS) was formed in response to that expressed need and was incorporated in early 2001. The PCIS has membership of approximately 70 companies from all critical infrastructure sectors. The CIAO and the U.S. Chamber of Commerce jointly provide administrative support to the PCIS and the CIAO facilitates communications between the industry members of the PCIS and their federal sector counterparts.

The PCIS also engages other stakeholders in critical infrastructure protection issues, including the risk management (audit and insurance), investment, and mainstream business communities. The PCIS is organized by industry, for industry, with the U.S. Government acting as a catalyst and a participant. Major topics being addressed by the partnership include approaches to addressing interdependency vulnerabilities, multi-sector information sharing, legislative and public policy issues, research and workforce development, industry participation in preparing the national strategy for critical infrastructure protection, and outreach to state and local governments.

Outreach to the Business Community

In FY 2001, the CIAO developed a roadmap of Chief Executive Officer (CEO)-centric organizations and established new relationships with the Business Roundtable, the Conference Board, and the American Business Conference. The CIAO also solidified its existing relationship with the National Association of Manufacturers. CIAO officials met with these organizations to discuss how best to increase awareness of critical infrastructure protection issues among these organizations' members and to develop a strategy for communicating with key business leaders. Additionally, the CIAO briefed members of the Business Roundtable in a larger public forum on the activities of the CIAO, homeland security, and private sector responsibility in preventing terrorist acts or disruptions to their critical services. These ongoing efforts are designed to change the culture of business to accept critical infrastructure assurance as a business issue and to raise the importance of the matter to the most senior levels within companies. The events of September 11 have accelerated many of these initiatives by highlighting the need to avoid disruptions of critical infrastructures.

The risk management community, including audit and insurance professionals, is also influential in bringing critical infrastructure protection issues to the forefront of corporate governance. The CIAO continued its outreach programs to auditors with a series of six "audit summits" across the country sponsored by an audit community consortium and led by the Institute of Internal Auditors (IIA) and the CIAO. These summits consisted of seminars that educated directors of corporate boards and chief auditors on their emerging responsibilities for overseeing prudent management of information security risks within their institutions. To make these summits as relevant and useful as possible, the CIAO, in combination with the National Association of Corporate Directors and the audit community, brought together participants from Wall Street, the insurance community, and the legal profession. As part of this partnership, the audit community published three booklets providing oversight guidance to corporate directors and auditors.

The outreach work with the audit community has now entered its third phase. In September 2001, in partnership with IIA, a CIAO team began providing two- and four-hour educational presentations to the majority of audit chapters across the United States. In the future, similar presentations may be given in other countries as well. IIA alone has approximately 150 chapters. These briefings are intended to help auditors understand the issue of critical infrastructure protection and give them tools to educate their own institutions and communicate specifically with their senior management and boards on these issues. The CIAO created reference materials that include guidance documents developed as a result of the audit summits, examples of the business case for action, and other resources and tools to inform auditors about standards development, information sharing activities, information security practices, benchmarking, analysis, and warnings of cyber attacks.

The audit summits produced additional outreach partnerships that help to raise awareness of critical infrastructure protection issues by showing how information security is a business issue and a matter of prudent management practice. One of these new partnerships was with the National Association of Corporate Directors (NACD). The NACD, in conjunction with the CIAO, is developing a tool for directors to use in performing their oversight duties over information security. That document will be

sent to NACD's membership in October 2001.

The CIAO also continued a highly successful awareness building partnership with CXO Media during FY 2001. This partnership emerged out of the CXO Media representative's attendance at the first audit summit. CXO Media publishes the *CIO Magazine* that represents the only direct professional conduit for good management practices for Chief Information Officers (CIOs). CXO Media set aside sessions addressing critical infrastructure protection in each of its six annual executive conferences, where the CIAO provided speakers for audiences of up to 400 CIOs from Fortune 500 companies. Together with the CIAO, CXO Media also developed and held two highly successful policy forums on information security and privacy, the most recent taking place in March 2001 in conjunction with the PCIS annual meeting. The CIAO also plans to establish a Public Affairs office to coordinate communication with the media and effectively carry its message to the public.

The CIAO initiated a relationship with the American Corporate Counsel Association (ACCA), whose members represent most of the Fortune 1000 firms. Potential activities with the ACCA include publishing articles in the ACCA newsletter, providing educational briefings for chapters, developing a business case for action for corporate legal counsels, increasing access to directors of boards who may have an interest in carrying the message, and participation of members in other meetings that will help advance the dialogue on critical infrastructure protection, especially on legal issues within a corporate counsel's purview. Activities with the ACCA represent an important channel of influence to corporate boards of directors and to senior corporate management.

CIAO officials also briefed the securities analysts of Salomon Smith Barney in FY 2001 on critical infrastructure protection issues. As part of our outreach efforts to financial analysts, Salomon Smith Barney sent their senior equity strategist to most of the audit summits to deliver remarks from a paper written on the connection between shareholder value and managing information security risk. Subsequently, the President and CEO of the Chicago Mercantile Exchange became a "champion" of the issue, commissioning a study within his own organization and speaking publicly about the results.

The CIAO also began a new state and local initiative to solicit input on the national strategy and to increase awareness of critical infrastructure issues at the community level among key associations, such as the National Governor's Association and the Council of Mayors. Further, the CIAO talked with representatives from several states (e.g., Kansas, Iowa, Georgia, Texas, and others), who volunteered to help provide input into the state and local section of the national strategy.

Briefings in FY 2001 by the CIAO staff to one of the Small Business Advisory Councils to the Department revealed a great deal of interest in critical infrastructure protection from owners of small businesses. From their perspective, reliable and available infrastructure services represent a critical foundation for operational survivability of small businesses. Small businesses have far fewer resources to recover or protect themselves when there is a disruption to their basic services. Consequently, they have far more to lose if such services are disrupted. A roadmap of key small business organizations will be developed to identify the most productive means of reaching out to small business leadership and channels of influence.

Finally, the CIAO's outreach team developed a roadmap of the key bureaus within the Department to raise awareness of critical infrastructure policy, with the potential to develop partnerships on outreach to business communities with whom the Department may already have a relationship. The CIAO met to discuss areas of commonalities with the E-Commerce Office within the International Trade Administration, and is pursuing a future relationship with that office. The CIAO continues working relationships with the National Telecommunications and Information Administration (NTIA) and the Technology Administration's National Institute of Standards and Technology (NIST). NTIA works with the information and communication sector and NIST contributes significantly to standards development and research.

Support for Federal Lead Agencies

Due to its experience with outreach programs, the CIAO also provided support for the federal lead agencies and their counterparts in industry for outreach and awareness building, specifically through the sponsorship of workshops on common issues shared by many of the sectors (e.g., risk management approaches, information sharing, legal obstacles). It also has provided support for the building of an industry-specific "business case for action," since the business cases for senior leadership in industry tend to center around common concerns such as business operational survivability, customer relationships, and investor and public confidence.

Project Matrix

Project Matrix was established in 1999 to assist federal departments and agencies in identifying critical assets and systems as well as key interdependencies essential to allowing the Federal Government to meet its responsibilities for protecting the nation's security and economy, and the health, welfare, and safety of U.S. citizens.

The results of Project Matrix enable each participating federal department or agency to:

- identify the nodes and networks that should receive robust cyber and physical vulnerability assessments;
- conduct near-term risk management assessments;
- justify funding requests for high-priority security enhancement measures in the areas of physical security, information system security, industrial security, emergency preparedness, counter-intelligence, counter-terrorism; and
- review actual business processes to better understand and improve the efficiencies of their organizations' functions and information technology architectures.

Project Matrix involves a three-step process. In Step 1, the Project Matrix team identifies and ranks the most critical assets of each federal department and agency. In Step 2, the team provides a business process topology on, and identifies significant points of failure associated with, each department or agency's most critical assets. In Step 3, the team identifies the infrastructure dependencies associated with each department or agency's most critical assets.

Project Matrix has solicited the voluntary participation of 17 civilian federal departments and agencies. A "discovery phase" review is typically conducted before Step 1 is initiated to verify that a given federal department or agency should participate fully in Project Matrix. The Project Matrix team also presently is documenting its entire analytical process for potential use throughout the public and private sectors, improving its automated data collection capabilities, and beginning to establish a master crisis management database system for use by the national security community.

Coordinating Education, Awareness, and Training

The United States needs an information-literate work force that is aware of its personal responsibility to employ good cyber security practices, as well as a cadre of information security professionals who are knowledgeable of the recognized "best practices" available in information security and information assurance. The National Colloquium for Information Systems Security Education (the Colloquium) was established to serve as a forum to bring government, industry, and academia together to meet those challenges. The CIAO serves on the Board of the Colloquium.

The Colloquium provides a round table forum to discuss and develop guidance for information security undergraduate and graduate academic curricula; common requirements; specific knowledge, skills, and abilities; certification requirements; and establishment of professionalization boards.

The 5th National Colloquium, held in May 2001 at George Mason University, greatly expanded participation among government, industry, and academia and strengthened these working partnerships by sharing the current trends in information security tools and techniques, including international perspectives. Both Australia and Great Britain made presentations on their educational programs at the conference. Increased numbers of academic institutions participated in an "information assurance boot camp" that included a strong awareness/background module and then provided information security education resources made available by Colloquium members with nationally recognized information assurance programs. As an outcome of the Colloquium, information assurance curricula were added to student studies in more universities than in past years.

The Federal Cyber Services (FCS) training and education initiative was designed to ensure an adequate supply of highly skilled federal information system security specialists entering federal service. Representatives of the CIAO, the National Security Council, the National Security Agency, the National Science Foundation (NSF), and the Office of Personnel Management developed a component of the FCS, the "Scholarship for Service" program, that was funded for FY 2001 in the NSF appropriation. The program offers grants to universities to build capacity for information assurance education, and also offers scholarships for students for up to two years in exchange for a commitment

to an equal amount of service to the Federal Government. Over 30 students accepted scholarships for fall 2001 and committed to working for the Federal Government upon graduation. Seven capacity-building grants were awarded to universities and professors in FY 2001.

The CIAO also actively works with working committees of the Federal Chief Information Officers Council (CIO Council), comprised of CIOs of the largest federal departments and with the Federal Information System Security Education (FISSEA), to share information. Federal CIOs protect the privacy and availability of the data on federal information systems. During FY 2001, the CIO Council working committees and the FISSEA developed and compiled recommended security practices, suggested criteria for evaluating federal security programs, shared security awareness material, and hosted several seminars and conferences to increase awareness of security issues, minimize interruption of government services, maintain privacy, and protect sensitive and national security classified information. Through these efforts, senior government executives are kept informed about developing information security issues and can exchange information on techniques for dealing with information technology security risks.

Development of the National Strategy

The CIAO had lead responsibility for developing version 1.0 of the *National Plan for Information Systems Assurance*. The plan, released in January 2000, focused on the Federal Government's efforts to improve information systems protection. During FY 2001, the CIAO worked with other agencies and the private sector to coordinate the development of the next plan. The next plan will be developed jointly between government and industry as an exercise for arriving at a consensus about respective roles and responsibilities. The purpose of the plan is to present an integrated public-private strategy for government and industry to chart a common course toward achieving the overall goal of national critical infrastructure assurance.

This plan will serve not only as a guide for action, but also as a vehicle for creating consensus in Congress and the public on how to proceed. A national strategy will also help to establish a foundation with the Congress and the public for proposing legislative and public policy reforms where such reforms are needed to advance national policy.

Return to Table of Contents