# Critical Infrastructure Protection: The Department Can Enhance Its International Leadership and Its Own Cyber Security

Report Number 01-IT-R-044, June 2001

# Table of Contents

# Executive Summary

## Purpose

The Office of Inspector General (OIG) assessed the Department of State's (Department's) progress in carrying out its Presidential Decision Directive (PDD)[1] 63 responsibilities for cyber critical infrastructure protection (CIP) during fiscal years 1998-2000.

Our objectives were to assess the Department's:

- Foreign Affairs Lead Agency activities under PDD-63;
- Critical Infrastructure Protection Plan (CIPP) development and implementation;
- minimum-essential cyber infrastructure vulnerability and risk assessments; and
- risk mitigation, emergency management, interagency security, resource requirements, and awareness and training policies and practices.

We identified additional steps the Department can take to address its PDD-63 Foreign Affairs Lead Agency and minimum-essential cyber infrastructure[2] responsibilities.

We conducted the review in conjunction with a President's Council on Integrity and Efficiency assessment of PDD-63 implementation at several Federal departments and agencies.

## Background

President Clinton issued PDD-63 to establish a national effort to ensure the security of the critical infrastructure of the United States.[3] Under PDD-63, the Department is responsible for protecting those of its facilities, people, and systems that it deems essential to national critical infrastructure, and for being the Foreign Affairs Lead Agency.

---

[1] Presidential Decision Directives were renamed National Security Presidential Directives after we finished our review.

[2] Minimum-essential cyber infrastructure supports core mission processes, which support national security and government continuity.

[3] Critical infrastructure consists of physical and cyber systems and assets that are so vital to the United States that their incapacity would debilitate national security, national economic security, or national public health and safety.

The Under Secretary for Management designated the Assistant Secretary of International Narcotics and Law Enforcement Affairs (INL) to be the Foreign Affairs Functional Coordinator. The Coordinator subsequently chaired the Subgroup on International Cooperation of the National Security Council (NSC) Critical Infrastructure Coordination Group.[4] The Subgroup is a forum for U.S. Government agencies to use in assessing and responding to international CIP issues.

Internally, the Under Secretary for Management established three organizations to address PDD-63 – the Virtual Governance Board, the Vulnerability Assessment Working Group,[5] and the Security Infrastructure Working Group. These organizations coordinate and implement the CIPP, the Integrated Systems Security Management Plan, and the Comprehensive Risk Management Plan, respectively.

## Results in Brief

PDD-63 directs the Department as Foreign Affairs Lead Agency to implement an international outreach strategy to safeguard U.S. and global critical infrastructures upon which the U.S. depends. The Department's Foreign Affairs Functional Coordinator started by issuing an international outreach plan in August 2000. The plan focuses on addressing international law enforcement issues involving a few countries. Although this focus on catching cyber terrorists and criminals is a commendable beginning, the approach does not address the PDD-63 principles of encouraging friendly and like-minded nations, international organizations, and multinational corporations to focus on global preventative measures.

During February and April 1999 the Department issued its CIPP and started its vulnerability assessment process, respectively. The CIPP contains 11 objectives, which address PDD-63 require-

[4] President Bush reconstituted the Critical Infrastructure Coordination Group and three other groups into the NSC Policy Coordination Committee on Counter-Terrorism and National Preparedness after we completed our review.

[5] The Department established the Vulnerability Assessment Working Group in February 1999, with responsibilities for identifying minimum-essential processes, core processes, and critical resources. The Chairperson for the Vulnerability Assessment Working Group is a representative of the Bureau of Diplomatic Security.

ments for minimum-essential infrastructure, vulnerability assessments, risk analysis and remediation, warning systems, response capabilities, reconstitution plans, and education and awareness programs. Although the Department has established a workable framework for protecting its minimum-essential infrastructure, its CIPP and vulnerability assessment process fall short of what PDD-63 requires.

## Principal Findings

### Foreign Affairs Lead Agency

#### Strengthening International Critical Infrastructure Protection

The Subgroup on International Cooperation of the NSC Critical Infrastructure Coordination Group has embraced a limited strategy focusing on the extent to which the United States depends on the infrastructure, economy, or government of other countries. PDD-63 states that the United States will promote international cooperation to help manage the worldwide CIP problem through joint responsibility among like-minded and friendly nations, international organizations, and multinational corporations. It further states the Federal Government must focus on preventative measures, and threat and crisis management, to provide maximum feasible security for at risk infrastructures.

Although worldwide cooperation is often difficult, the United States could provide broader CIP leadership because of its greater experience and expertise in addressing cyber security issues. Such an effort could include encouraging the Department's missions, other Federal agencies, international trade and business groups, and multilateral international organizations to seek ways to strengthen the CIP of other countries through preventative measures.

#### Law Enforcement Assistance

The countries we visited are strengthening their cyber criminal laws, investigation and prosecution organizations, and international ties for conducting investigations. However, law enforcement officials face two major problems in conducting international investigations. First, criminal laws and procedures vary among countries. Second, obtaining support from foreign law enforcement agencies is often difficult and time consuming. The Department, as the Foreign Af-

fairs Lead Agency, could enhance the positive efforts of other countries to fight cyber crime by assisting friendly and like-minded foreign law enforcement organizations obtain additional cyber training and technical assistance, and by helping establish improved international communication channels for processing requests for assistance and access to evidence.

## Critical Infrastructure Protection Plan

### Department's Foreign Operations

The Department's CIPP and vulnerability assessments did not address the Department's minimum-essential infrastructure overseas, nor the role and responsibilities of its Chiefs of Mission in protecting that infrastructure. Foreign operations are essential to U.S. Government foreign policy and relations, national defense, and U.S. interests abroad.

### Periodically Assessing Security Controls

PDD-63 requires periodic review of the reliability, vulnerability, and threat environment of minimum-essential cyber infrastructure to ensure organizations are addressing changing technology and threats with appropriate protective measures and responses. Office of Management and Budget (OMB) Circular No. A-130, Appendix III requires all Federal agencies evaluate the security controls of all their automated information systems at least once every 3 years. Because the Department's CIPP and related policies do not address this requirement, it has not developed a schedule for testing minimum essential cyber infrastructure for security controls vulnerabilities.

### Critical Interagency Systems Vulnerabilities

The National Plan for Information Systems Protection, promulgated by President Clinton last year, has a focus on shared cyber security interdependencies and vulnerabilities among agencies. The Department's vulnerability assessment did not address the cyber security interdependencies and vulnerabilities it shares with other organizations.

### Security awareness and training policies, practices, and procedures

The Department had not complied with Computer Security Act of 1987 and related Federal policies that mandate annual security awareness, training and education for employees in accepted security practices relevant to their individual roles and responsibilities. Implementing well-organized approaches to ensuring all employees receive required security awareness, training and education when required will strengthen the Department's security readiness.

## Recommendations

### Foreign Affairs Lead Agency

We recommend the Foreign Affairs Functional Coordinator, with assistance from the Department's International Information Programs Coordinator, take the following steps:

- encourage multilateral cooperation, contingency planning, and open exchange of public information with a wide range of friendly and like-minded countries, international organizations, and multinational corporations;
- provide bureaus and posts with public information to assist friendly and like-minded foreign governments in strengthening their CIP; and
- emphasize encouraging and coordinating the efforts of other U.S. Government lead agencies in informing and assisting a wide range of friendly and like-minded countries to better defend themselves against cyber attacks.

### Critical Infrastructure Protection Plan

We recommend that:

- The Chief Information Officer and the Assistant Secretary for Diplomatic Security address the Department's foreign operations in subsequent critical infrastructure protection plans and vulnerability assessments. In doing so, other agencies with overseas presence should be included in developing the overseas portion of the plans, and conducting and assessing the overseas portion of the vulnerability assessments as appropriate.

- The Assistant Secretary for Diplomatic Security schedule and conduct security controls evaluations of all minimum-essential cyber infrastructures at least once every 3 years as required by OMB Circular No. A-130, Appendix III for all automated information systems.
- The Assistant Secretary for Diplomatic Security amend 12 Foreign Affairs Manual (FAM) 600 and the Bureau of Information Resource Management (IRM) amend the critical infrastructure protection plan to require security control evaluations of minimum-essential cyber infrastructure at least once every 3 years.
- The Chief Information Officer and the Assistant Secretary for Diplomatic Security ensure that subsequent critical infrastructure protection plans and vulnerability assessments address minimum-essential interagency infrastructure vulnerabilities.

### Employee Security Awareness, Training and Education

We make 10 recommendations, principally to the Assistant Secretary for Diplomatic Security, to conform the Department's employee security awareness, training and education policies, practices, and procedures, as stated in 12 FAM 600, with all relevant requirements of the Computer Security Act of 1987 and related U.S. Government policies.

## Department Comments

We provided the relevant Bureaus with a draft of this report for their review and comments. Generally, the Bureaus agreed with our report's findings and recommendations. However, in response to the Bureau of International Narcotics and Law Enforcement Affairs concerns that the report did not properly characterize the Department's international outreach strategy, we added information to support the need for a broader strategy addressing global critical infrastructure protection. The comments of the bureaus are addressed in the Findings Section of the report, and included in their entirety in Appendix E through H.

# Purpose and Scope

We conducted this review to assess the Department's progress in meeting its PDD-63 responsibilities, as they relate to minimum-essential cyber infrastructure.[6] We assessed the Department's:

- Foreign Affairs Lead Agency activities under PDD-63,
- Critical Infrastructure Protection Plan development and implementation;
- minimum-essential cyber infrastructure vulnerability and risk assessments; and
- risk mitigation, emergency management, interagency security, resource requirements, and awareness and training policies and practices.

We conducted the review in conjunction with an assessment of PDD-63 implementation by the President's Council on Integrity and Efficiency at several departments and agencies.

We did not test the Department's information security controls during this evaluation, but instead relied on the results of earlier reviews (see Appendix B). Because the vulnerability remediation process was incomplete at the end of our review, we could not assess whether it was used to establish and fund the most critical priorities.

We interviewed officials in the Department's Office of the Under Secretary for Management, Bureau of Diplomatic Security (DS), IRM, INL, Bureau of Intelligence and Research, International Information Programs, geographic bureaus, Foreign Service Institute, and Diplomatic Telecommunications Service regarding their involvement with the preparation and execution of the Department's CIPP. We also interviewed officials at the National Critical Infrastructure Assurance Office, Department of Defense, Central Intelligence Agency, and Director of Central Intelligence Center for Security Evaluation regarding relevant aspects of the CIPP and the Department's role as the Foreign Affairs Lead Agency under PDD-63.

---

[6] The Department conducted vulnerability assessments of only those assets whose loss would limit the Department's capability to perform minimum-essential processes and that are an essential part of our nation's "minimum-essential" infrastructure.

During May and June 2000, we performed work at the U.S. Embassies in Tokyo and London, and the American Institute in Taiwan, where we met with U.S. Government, host government, and private sector officials. We selected those locations because the governments and private entities in those countries were addressing cyber threats to their critical infrastructure, and were in a position to assess what role the U.S. Government might play in addressing international cyber security issues.

We followed generally accepted government auditing standards and conducted such tests and procedures, as we considered necessary for the assignment. Staff from our Information Technology Issue Area performed this evaluation from March 2000 through February 2001. Frank Deffer, Acting Assistant Inspector General; Robert C. Taylor, Audit Manager; John Shiffer and Anthony Carbone, Senior Auditors contributed to the report. Mr. Deffer, at defferf@state.gov and 703.284.2715, or Mr. Taylor at taylorr2@state.gov and 703.284.2685, will respond to comments or questions about the report.

# Background

In October 1997, the President's Commission on Critical Infrastructure Protection reported[7] that the information revolution and the introduction of computers into virtually every dimension of our society had changed our economy, national security, and everyday lives. In particular, many of our most sophisticated global national security systems rely on commercial power, communications, and transportation, which are also computer-controlled.

The Commission found that all computer-driven systems are vulnerable to intrusion and destruction. A concerted attack on the computers of any one of our essential economic sectors or governmental agencies could have catastrophic effects. The Commission also found that the threat was real. Where once our enemies mostly relied on bombs and bullets, they can now use computers to inflict enormous damage. The Commission concluded that to preserve our security and economic well being, we must protect our critical computer-controlled systems from attack, and assist friendly and like-minded countries protect their critical cyber infrastructure.

After reviewing the Commission's report, President Clinton issued Presidential Decision Directive 63 in May 1998 to establish a national effort to ensure critical infrastructure security, also known as minimum-essential infrastructure, for the United States and other friendly countries.[8] On April 5, 2001, the Director of the National Critical Infrastructure Assurance Office testified before The House Commerce Committee, Subcommittee on Oversight and Investigations, that President Bush has indicated critical infrastructure protection will be a priority of his administration.

---

[7] Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, Washington, DC, October 13, 1997.

[8] The PDD-63 White Paper defines critical infrastructure as the " . . . physical and cyber-based systems essential to the minimum operations of the economy and government." The Critical Infrastructure Assurance Office defined agency minimum-essential infrastructure as the organizations, personnel, systems, and facilities required to accomplish an agency's core mission as its mission relates to national security, national economic security, or continuity of government services.

PDD-63 requires Federal agencies to assess the cyber vulnerabilities of the Nation's critical infrastructures — information and communications, energy, banking and finance, transportation, water supply, emergency services, and public health — and the authorities responsible for the continuity of federal, state, and local governments. The directive places special emphasis on protecting the government's own critical assets from cyber attack and the need to remedy deficiencies in order to become a model of information security. The directive also calls for the Federal Government to produce a detailed plan to protect and defend America against cyber disruptions. PDD-63 acknowledges that CIP encompasses a wide range of information infrastructure security, strategy, and policy issues that we share with other countries on a regional and global basis. The United States is to take all necessary measures to eliminate significant CIP vulnerabilities within its borders, especially those involving cyber attacks, by May 22, 2003.

PDD-63 requires the Department to protect those of its facilities, people, and systems essential to U.S. critical infrastructure, and to be the U.S. Government Foreign Affairs Lead Agency.[9] Further, the Omnibus Diplomatic Security and Antiterrorism Act of 1986 requires the Secretary of State to develop and implement security-related policies and programs for U.S. Government diplomatic operations. The Department's security policies and programs are supposed to ensure the security of all U.S. Government personnel on official business overseas and all facilities overseas for which the Secretary of State is responsible.

## Foreign Affairs Lead Agency

PDD-63 asserts that because the U.S. Government shares responsibility with the governments of other countries for global CIP, Federal agencies shall encourage international cooperation in managing the global CIP problem. The Undersecretary for Management selected the Assistant Secretary of INL to be Foreign Affairs Func-

[9] The lead agencies are supposed to encourage and support their private and public sector counterparts to develop awareness, vulnerability assessment, and information sharing initiatives. They include telecommunications, banking and finance, energy, transportation, and essential government services.

tional Coordinator. The Coordinator is responsible for fostering international CIP cooperation, directing departmental and interagency efforts across the range of international CIP issues, and coordinating all U.S. Government foreign affairs activities.

The NSC Critical Infrastructure Coordination Group tasked its Subgroup on International Cooperation, chaired by the Assistant Secretary of INL, to assess international CIP issues and respond with global solutions. In August 2000, the Subgroup issued an international CIP outreach strategy report prepared by the Foreign Affairs Functional Coordinator.

## Critical Infrastructure Protection Plan

The National Critical Infrastructure Assurance Office issued the National Plan for Information Systems Protection in January 2000 as called for by PDD-63. The Plan proposes 10 programs for achieving the objectives of (a) preparing for and preventing intrusions, (b) detecting and responding to intrusions, and (c) building strong cyber security foundations.[10]

The Department issued its CIPP and started its vulnerability assessment process in February and April 1999, respectively, because it already had the benefit of an extensive body of information assurance policies, procedures, and programs. Several OIG, DS, and General Accounting Office reports indicating the nature and scope of the Department's cyber security vulnerabilities were also available.

The Under Secretary for Management delegated to the Chief Information Officer (CIO), responsibility for protecting the Department's cyber systems, and delegated to the Assistant Secretary for DS, as the Chief Infrastructure Assurance Officer, responsibility for overseeing protection of the remaining critical infrastructure. The Under Secretary for Management also established the Virtual Governance Board, Vulnerability Assessment Working Group, and Security Infrastructure Working Group to coordinate and implement the CIPP, the Integrated Systems Security Management Plan, and the Comprehensive Risk Management Plan.

---

[10] Preparing for, preventing, detecting and responding to intrusions addresses critical infrastructure assets, shared interdependencies, and vulnerabilities by minimizing the possibility of significant attacks on national critical infrastructure, and building an infrastructure that remains effective when attacked.

The CIPP describes the Department's plans to reduce risks to minimum-essential cyber infrastructure and other mission critical cyber systems. At the time of our review, the Department had:

- defined minimum-essential infrastructure, identified domestic minimum-essential cyber and physical infrastructure security vulnerabilities and initiated risk assessments to determine how best to address the vulnerabilities;
- established an organizational structure for developing CIP priorities and funding;
- implemented an intrusion detection system to detect and respond to cyber attacks;
- prepared a critical infrastructure reconstitution[11] plan in case of successful infrastructure attacks; and
- established a cyber security awareness program and shared cyber threat intelligence with other agencies.

[11] A system to reconstitute minimum required capabilities for varying levels of successful infrastructure attacks in a rapid manner.

# Findings

The Department can do more to enhance the results of its efforts to carry out its Foreign Affairs Lead Agency role and to address the minimum-essential cyber infrastructure requirements of PDD-63.

The international outreach strategy developed by the Subgroup on International Cooperation under the Department's leadership emphasizes international law enforcement consultations with a few close allies. In contrast, PDD-63 encourages international CIP cooperation with like-minded and friendly nations, international organizations, and multinational corporations and a focus on preventative measures as well as threat and crisis management. The Department's International Information Programs Coordinator should assist the Subgroup on International Cooperation expand and enhance the strategy to include encouraging a wide range of like-minded and friendly governments to implement effective CIP measures.

The Department's CIPP has 11 objectives addressing PDD-63 requirements for minimum-essential infrastructure, vulnerability assessments, risk analysis and remediation, warning systems, response capabilities, reconstitution plans, and education and awareness programs. Although the plan provides a suitable framework for protecting minimum-essential cyber infrastructure, it falls short of what PDD-63 requires.

## Foreign Affairs Lead Agency

The President's Commission on Critical Infrastructure Protection wrote in its 1997 report, *Critical Foundations: Protecting America's Infrastructure* that the United States is in the vanguard of countries to deal with international CIP. The Commission concluded that the status of the United States gives it the opportunity to shape international cooperation and positively influence governments and infrastructure owners and operators who share our global community. Achieving the Commission's goal will require substantial international collaboration beyond the limitations of the existing international outreach strategy.

The situation described by the President's Commission still exists according to the Director of the National Infrastructure Protection Center. On April 5, 2001, the Director testified before the

House Energy and Commerce Committee, Oversight and Investigations Subcommittee, that information warfare against the critical infrastructures of the United States and other nations is perhaps the greatest cyber threat to our national security. He further testified that terrorists groups are using cyber technology for planning, fund raising, propaganda, and secure communications, and that foreign intelligence services have adapted cyber tools to their information gathering tradecraft.

In combating this situation, PDD-63 requires the U.S. Government to encourage international cooperation to help manage the global CIP problem and to focus its efforts on preventative measures and threat and crisis management involving like-minded and friendly nations, international organizations, and multinational corporations. The NSC Critical Infrastructure Coordination Group designated the Subgroup on International Cooperation, chaired by the Foreign Affairs Functional Coordinator, to coordinate these efforts.

Under the direction of the Subgroup on International Cooperation, and following interagency discussions and consultations, the Foreign Affairs Functional Coordinator published a classified plan, CIP: A Four Track Approach to International Outreach,[12] in August 2000. The plan provides guidance and procedures for coordinating U.S. Government international CIP activities. Priorities for cooperation with other countries are governed by the extent to which the U.S. depends on the infrastructure of the other countries or groups of countries. Although the document discusses promoting CIP awareness and security standards, it emphasizes law enforcement as key to dealing with global minimum-essential cyber infrastructure security. Further, the document contains no discussion of preventative protective measures the U.S. Government should take to enhance international CIP.

The document places minimal emphasis on developing global solutions by expanding cooperation on CIP preventative measures with like-minded and friendly nations, international organizations, and multinational corporations, as envisioned by PDD-63. As suggested by the President's Commission on Critical Infrastructure Protection, the most effective and efficient method for achieving

[12] See Appendix D for an unclassified summary of the strategy.

increased protection from cyber threats involves a strategy of cooperation and information sharing among infrastructure owners and operators and relevant government entities. In addition, the Commission pointed out the need for comprehensive awareness and education programs at all levels of society.

INL officials told us resource constraints and national security concerns cause this lack of emphasis on a wider global effort. However, according to the Department's International Information Programs Coordinator, it already has resources available to assist the Subgroup on International Cooperation of the NSC Critical Infrastructure Coordination Group in developing a broad outreach program as envisioned by PDD-63. Presumably, the Department would implement such efforts within appropriate national security constraints.

## Strengthening International Critical Infrastructure Protection

Compared to the approach described in PDD-63, the Subgroup on International Cooperation of the NSC Critical Infrastructure Coordination Group has adopted a constrained strategy for strengthening international CIP.

PDD-63 directs the Federal Government to take a global and preventative approach to expanding CIP cooperation among like-minded and friendly nations, international organizations, and multinational corporations without any stated limit on the extent of our critical infrastructure interdependencies. PDD-63 is not in any way focused on regulating the use of global information technology and systems. This approach recognizes that, in cyber-space, the United States is interdependent with a wide range of countries, and that globally shared responsibility and partnership among critical infrastructure owners and operators and governments, not additional regulations, are key to the success of international CIP.

The Subgroup on International Cooperation chose, however, to constrain its strategy to focusing on the extent to which the United States is dependent on the infrastructure, economy, or government of a hand full of other countries. The highest priorities of the strategy are on bilateral, interagency, and sector specific CIP work

with strategic partners and a few international organizations[13] with the goal of jointly regulating the use of global information technology and systems. The first priority countries are those that the United States has the greatest degree of infrastructure interdependency. The second priority countries are those with which we have limited infrastructure interdependencies but significant economic and governmental interdependencies and opportunities for cooperative efforts. The lowest priority is on bilateral and multilateral CIP awareness-raising activities involving a broad range of friendly and like-minded countries and regional groups as described in PDD-63.

The Subgroup on International Cooperation could initiate a more substantial international CIP collaboration effort by having the lead agencies for all sectors provide the Department's geographic bureaus and posts with public sector-specific CIP material, and lists of contacts that their foreign counterparts can access for CIP awareness, technical assistance and training.[14]

Further, the Department's International Information Programs Coordinator is available to facilitate international CIP outreach and cooperation.[15] Under the collaborative guidance of the Coordinator and the Subgroup on International Cooperation, posts could sponsor host country, sector specific, and regional working groups that include representatives of host country government and private entities and international organizations,[16] in order to share CIP information. An International Information Programs Coordinator

---

[13] For example, the United Nations, North Atlantic Treaty Organization, G 8, Council of Europe, Asian Pacific Economic Council, and Organization of American States.

[14] An example involved the Department and several Federal agencies in the Year 2000 International Interagency Working Group. They reviewed Year 2000 preparations overseas and assisted dozens of countries.

[15] Such an effort would be similar to the global public diplomacy campaign, led by the former U.S. Information Agency that addressed host country and cross-border Year 2000 issues.

[16] In 1999, posts formed working groups with the embassies of other countries to discuss Year 2000 issues among themselves and with host country representatives. This was an effective method for exchanging information and coordinating contingency planning.

representative said the office could facilitate a variety of CIP outreach efforts, if requested by the Foreign Affairs Functional Coordinator on behalf of the Subgroup on International Cooperation.[17]

Although global cooperation on such technically complex issues is often difficult, officials in the countries we visited said the United States could provide global CIP leadership because of its cyber security experience and expertise and suggested the United States could play an active role in increasing global CIP awareness, technical assistance, and training.

Recommendation 1: We recommend the Assistant Secretary for International Narcotics and Law Enforcement Affairs, acting as the Foreign Affairs Functional Coordinator, seek to have the National Security Council Policy Coordination Committee on Counter-Terrorism and National Preparedness, which incorporates the Subgroup on International Cooperation of the NSC Critical Infrastructure Coordination Group, expand its approach to international critical infrastructure protection. This approach should include:

- coordinating the efforts of U.S. Government sector leaders to provide critical infrastructure protection information and assistance to a wide range of friendly countries requesting such assistance;
- focusing the efforts of U.S. Government sector leaders, Department missions, trade and business groups, and international organizations on actively promoting critical infrastructure protection preventative measures;
- encouraging multilateral cooperation, contingency planning, and open exchange of public information with the widest possible range of friendly countries and international organizations;
- supporting Department of State posts in engaging foreign governments in joint efforts to prevent or otherwise solve critical infrastructure protection problems; and

[17] During Y2K preparations, the former U.S. Information Agency developed a readiness database for 16 critical infrastructure sectors in foreign countries. Posts supplied data using vulnerability and readiness criteria developed by the Year 2000 International Interagency Working Group chaired by the Department. A similar database of CIP vulnerability and readiness assessments would be useful for contingency planning by the Department and other agencies with an overseas presence.

- using the expertise and resources of the International Information Programs Coordinator in developing and implementing the Working Group's outreach efforts.

Comments by the Bureau of International Narcotics and Law Enforcement Affairs: In its written comments, the Bureau stated the draft report contains many helpful observations and suggestions. However, the Bureau also criticized this section of our report, stating that it mischaracterized the U.S. Government's international outreach strategy. The Bureau stated that PDD-63 directed the Subgroup to develop an international plan "as a subordinate and related task" to completing the first ever U.S. National Infrastructure Assurance Plan.

In our view, because the President issued the National Plan for Information Systems Protection, the subject of this report, 8 months before the international outreach strategy was developed, the Bureau had few constraints in how comprehensively it developed the international strategy

Our recommendation, if implemented, would enhance the international strategy by allowing the Department as a whole, and other public, private and nongovernmental organizations, to address PDD-63's explicit goals for the Federal Government to:

- protect the security of our globally linked domestic and international critical cyber infrastructure,
- encourage international cooperation to help manage "this increasingly global problem,"
- encourage market incentives and other actions to help harness the latest technologies to accomplishing "global solutions" to international problems,
- focus on preventative measures, and
- establish an international cooperation "plan to expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations and multinational corporations."

Comments by the International Information Programs Coordinator: The Acting Coordinator stated his organization is willing to assist in the type of international public information and assistance called for in this report. He noted, however, that such an effort would require the ongoing level of resources support the Department committed to addressing Y2K. We believe the Assistant Secretary for International Narcotics and Law Enforcement Affairs

should work with the Acting Coordinator to identify the resources needed for a sustained effort to broaden the international outreach strategy, and present the results of that analysis to the Subgroup on International Cooperation to include in the international outreach strategy.

Comments by the Bureau of Information Resource Management: The Chief Information Officer observed that information management officers and others at our posts are trained and experienced in critical information technology protection, and have experience in working with foreign organizations and governments in addressing information technology security issues. We agree with the Chief Information Officer that enlisting their assistance, just as the Department did most recently during our government's international Year 2000 preparations, could further the international cooperation goals of PDD-63.

## Law Enforcement Assistance

Growth in international cyber crime demonstrates the need for greater international law enforcement cooperation. Effectively responding to this threat requires that U.S. and foreign law enforcement authorities be able to overcome cultural, linguistic, legal and digital barriers that hamper the appropriate and timely exchange of criminal investigative information.

These issues were brought to the forefront at the July 26, 2000 hearing of the Subcommittee on Government Management, Information and Technology of the House Committee on Government Reform on *Computer Security: A War without Borders*. The Subcommittee Chairman noted that not all countries have the capability to detect and address international computer attacks. He further noted that even with countries that have law enforcement agencies and organizations that can investigate and share cyber-attack information, there is a question among the variety of players regarding who is coordinating an efficient, effective response to this international problem. The Subcommittee examined the challenges of coordinating these cyber-attack investigations.

In a similar vein, we found that although the law enforcement officials we met overseas were pleased with the assistance they received from the U.S. Government, they told us they need more help to enhance awareness and training at all levels of law enforcement, and improve the efficiency and scope of investigative assistance

that can be obtained from the large variety of law enforcement jurisdictions and organizations in the United States in order to obtain timely access to cyber evidence.

### Training and Technical Assistance

The countries we visited have strengthened their cyber criminal laws, investigative and prosecution organizations, and international ties for conducting investigations. They have participated in multilateral and bilateral efforts to address the problems, and have sent staff to the United States for bilateral discussions and training. Some countries and international organizations are establishing specialized units to address cyber crime in their countries. The European Union plans to issue guidelines to member countries for fighting cyber crimes including recommended cyber crime laws, and the G 8 is drafting recommended cyber crime laws and a cyber crime treaty for member countries.

Our government could enhance these positive efforts to fight cyber crime by providing additional training and technical assistance, especially to a wide range of friendly developed and developing countries. It does little good to strengthen laws and treaties if law enforcement officials and staff do not know enough about cyber technology to judiciously handle a wide range of cyber crime investigations and cases. Providing friendly countries with necessary expertise and materials to train officials and staff in the judiciary, prosecution, and police would go a long way to address these needs. For example, the Federal Bureau of Investigation Academy can provide investigative computer instruction, training, and curriculum for foreign law enforcement personnel.

Recommendation 2: We recommend the Assistant Secretary for International Narcotics and Law Enforcement Affairs, acting as the Foreign Affairs Functional Coordinator, work with U.S. Government and nongovernmental organizations to provide friendly foreign governments with opportunities for obtaining cyber law enforcement training and technical assistance.

Bureaus' Comments: The Bureaus did not comment on Recommendation 2.

## Investigative Assistance

Law enforcement officials in the countries we visited told us the two biggest problems in international investigations involve obtaining information, because legal criminal law and procedures vary among countries, and obtaining support from host country law enforcement agencies. For example, one of the major problems faced in dealing with Internet crime is obtaining timely access to useful information from foreign Internet service providers. The normal procedure for obtaining such information involves an international letters rogatory followed by a court order or subpoena, which can be a time-consuming process. However, with some types of computer crime, and specifically cyber intrusions, an immediate response is necessary by law enforcement, since data needed for evidence are generally only stored for a brief time period.

A possible solution to the investigative assistance problem was suggested by the Chief, Computer Crime Unit, Swedish National Crime Investigation Department, in his July 2000 testimony before the hearing on *Computer Security: A War without Borders* of the Subcommittee on Government Management, Information, and Technology. The Chief testified that the major problem his unit faces in coping with Internet crime is obtaining access to investigative information from foreign internet service providers and responsible web managers. Normally, providers request court orders, subpoenas or other formal domestic dispositions before they provide the requested information. Such requests involve time-consuming and difficult international letters rogatory. One way to address these problems, he suggested would be international agreements to release subscriber information and address logs to foreign law enforcement authorities without formal letter rogatory requests in a manner that ensured proper handling of the information.

The officials we met suggested establishing improved communication channels for more efficient and effective processing of investigative assistance requests and improved procedures for gaining access to evidence in a more timely manner. An example is setting up special communication channels that would be open 24 hours a day to handle urgent and critical cases. They also recommended governments give their central investigative agencies authority to act immediately to preserve evidence crucial to international cyber investigations.

Recommendation 3: We recommend the Assistant Secretary for International Narcotics and Law Enforcement Affairs, acting as the Foreign Affairs Functional Coordinator, work with the Department of Justice to identify and disseminate through posts more efficient and effective communications channels for processing foreign governments' investigative assistance requests, and improved procedures for gaining more timely access to evidence, that foreign law enforcement entities can use to enhance their investigations of cyber crimes involving United States entities and individuals.

Bureaus' Comments: The Bureaus did not comment on Recommendation 3.

## Critical Infrastructure Protection Plan

The Department established a CIPP with 11 objectives addressing the PDD-63 requirements for minimum-essential infrastructure, vulnerability assessments, risk analysis and remediation, warning systems, response capabilities, reconstitution plans, and education and awareness programs. Although the Department implemented several important parts of the plan for its domestic operations, and established a suitable framework for addressing its minimum- essential infrastructure, it excluded important elements from the CIPP and vulnerability assessment processes. Specifically,

- The Department has not assessed the vulnerabilities of its minimum-essential cyber infrastructure in its foreign operations.
- The Department's CIPP, policies, and procedures do not adequately address the OMB Circular No. A-130, Appendix III requirement to review the security controls of all automated information systems, including those that are part of its minimum-essential infrastructure, at least once every 3 years.
- The Department has not assessed vulnerabilities in its interagency connections.
- The Department's CIPP, policies, and procedures do not specify how the Department will ensure that all employees and contractors are trained on required CIP concepts and skills applicable to their respective involvement with the Department's minimum-essential cyber infrastructure.

- The Department's CIPP and associated policies do not require bureaus and posts to notify the Corporate Information System Security Officer of the designation of Information System Security Officers and their alternates.

## Department's Foreign Operations

The Department did not include foreign operations in its PDD-63 planning, and the CIPP and vulnerability assessments did not address the role of foreign operations in protecting minimum-essential infrastructure. Further, the Department did not consult the Director of Central Intelligence Center for Security Evaluation[18] during preparation of the CIPP and the vulnerability assessment regarding potential minimum-essential cyber security issues affecting the intelligence community abroad.

The Department provides minimum-essential cyber infrastructure support for its own operations and those of other U.S. Government agencies operating overseas. These overseas operations are essential to U.S. Government foreign policy and relations, national defense, and American interests abroad. The OIG has issued several reports on vulnerabilities in the Department's foreign cyber operations, including inadequate security of classified and unclassified systems. Whether the Department or the other agencies consider the overseas cyber infrastructure minimum-essential has not yet been determined.

Recommendation 4: We recommend the Chief Information Officer and the Assistant Secretary for Diplomatic Security address the Department's foreign operations in subsequent critical infrastructure protection plans and vulnerability assessments to determine what, if any, overseas minimum-essential cyber infrastructure should be subject to vulnerability assessments. In doing so, Department officials should include representatives of other agencies having an overseas presence in developing the overseas portion of the plans, and conducting and assessing the overseas portion of the vulnerability assessments as appropriate.

[18] This organization is responsible for protecting intelligence sources and methods information in U.S. Diplomatic facilities abroad based on its analysis of foreign intelligence vulnerabilities and countermeasures.

Comments of the Bureau of Information Resource Management: The Bureau of Information Resource Management concurred in Recommendation 4.

Comments by the Bureau of Diplomatic Security: The Bureau of Diplomatic Security agreed that this critical area requires PDD-63 assessment, and said the Department plans to address this recommendation during the next phase of its continuing PDD-63 vulnerability assessment process.

## Periodically Assessing Security Controls

PDD-63 requires frequent assessments of the reliability, vulnerability, and threat environment of minimum-essential cyber infrastructure so that organizations can address changing technology and threats with appropriate protective measures and responses. OMB Circular No. A-130, Appendix III requires evaluating the security controls of all automated information systems (presumably including minimum-essential cyber infrastructure) at least once every 3 years, and whenever there are significant changes to the systems.

Although DS planned to increase its evaluation activities, there is no supporting schedule or policy regarding minimum-essential cyber infrastructure. Further, the CIPP and Department policies make no reference to testing minimum-essential cyber infrastructure for security controls vulnerabilities at least once every 3 years as required for all cyber systems by OMB Circular No. A-130, Appendix III. DS has issued security software toolkits to identify inappropriate security configurations in unclassified systems, but none for minimum-essential cyber infrastructure.

We are recommending that DS evaluate cyber minimum-essential infrastructure security controls at least once every 3 years because that is the only Federal Government criteria at this time. However, we believe DS should consider more frequent testing of those controls given the very dynamic threat environment faced by the Department's cyber minimum-essential infrastructure, and the importance of that infrastructure to mission accomplishment.

Recommendation 5: We recommend the Bureau of Diplomatic Security schedule and conduct security controls evaluations of all minimum-essential cyber infrastructure at least once every 3 years, and whenever there are significant changes to minimum-essential cyber infrastructure, both as required by OMB Circular No. A-130, Appendix III.

Recommendation 6: We recommend the Bureau of Diplomatic Security modify 12 Foreign Affairs Manual 600, and the Bureau of Information Resource Management amend the Critical Infrastructure Protection Plan, to require periodic security control evaluations of all minimum-essential cyber infrastructure at least once every 3 years.

Comments by the Bureau of Diplomatic Security: The Bureau commented that it had periodically conducted penetration tests on the Department's networks, but that it will not conduct additional evaluations until December 2003. Although the Bureau is augmenting its capabilities, it recommended limiting periodic security controls evaluations to only those systems identified in the Vulnerability Assessment Reports.

Although we are pleased the Bureau is committing more resources to this effort, we are concerned that these resources will not be fully deployed until December 2003. It is not making an explicit commitment to meeting OMB Circular No. A-130, Appendix III requirements to schedule and conduct security controls evaluations once every 3 years, at least as they pertain to all minimum-essential cyber infrastructures. Regarding the Bureau's desire to limit the scope of the evaluations, we remind the Bureau that OMB Circular No. A-130, Appendix III requires such evaluations for all automated information systems in the Department.

Comments of the Bureau of Information Resource Management: The Chief Information Officer concurred with the recommendation to conduct security control evaluations periodically and whenever there are significant changes to minimum-essential cyber infrastructure. The CIO suggested we change the recommendation to conduct the evaluations more often, perhaps once every 18 months as in evaluations of secure communications (COMSEC) systems, because of the many changes in configurations and threats. We left it at 3 years as required by OMB Circular No. A-130, Appendix III.

## Critical Interagency Systems Vulnerabilities

The national minimum-essential information systems protection plan requires agencies to identify shared interdependencies and vulnerabilities. The plan focuses on minimum-essential systems that cross between agencies and are interdependent for their security.

The Department's vulnerability assessment did not address the potential impact on national minimum-essential infrastructure of its cyber connections with other agencies.

## Assessments of Interagency Minimum-Essential Infrastructure Vulnerabilities

The National Plan for Information Systems Protection prepared by the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism calls for agencies to identify their critical infrastructure system interdependencies and their associated shared threats and vulnerabilities. The Department did not assess the vulnerabilities in its minimum-essential cyber infrastructure relationships with other agencies. One example is that the Foreign Service National Pay System's direct connections to the Department of Treasury minimum-essential information systems may pose some risks to the Department of Treasury's minimum-essential cyber infrastructure.

Recommendation 7: We recommend the Chief Information Officer and Bureau of Diplomatic Security ensure that subsequent critical infrastructure protection plans and vulnerability assessments address minimum-essential interagency infrastructure vulnerabilities.

Comments of the Bureau of Information Resource Management: The Bureau of Information Resource Management concurred with Recommendation 7.

Comments by the Bureau of Diplomatic Security: The Bureau commented that the Department has developed plans to assess interdependencies with other agencies during subsequent phases of its vulnerability assessment activities. We anticipate those plans will be described in the next version of the Department's Critical Infrastructure Protection Plan.

## Interagency CIP Training and Exercises

PDD-63 generally and the Department's CIPP specifically requires the Foreign Service Institute to establish training and exercises involving interagency critical infrastructure protection practices and procedures using guidance provided by DS and IRM. However, DS

and IRM have not provided the Foreign Service Institute with the guidance it needs to develop the interagency CIP training and exercises required by PDD-63 and the Department's CIPP.

Recommendation 8: We recommend the Assistant Secretary for Diplomatic Security, Chief Information Officer, and the Director of the Foreign Service Institute jointly develop and implement interagency critical infrastructure protection practices and procedures training and exercises that meets the requirements of Presidential Decision Directive 63.

Comments by the Bureau of Diplomatic Security: The Bureau commented that the Vulnerability Assessment Working Group, in concert with the Bureau of Information Resource Management and the Foreign Service Institute, will identify opportunities to develop materials and courses to meet this requirement.

Comments of the Bureau of Information Resource Management: The Bureau of Information Resource Management concurred with Recommendation 8.

## Designations of Information System Security Officers and Alternates

The Omnibus Diplomatic Security and Antiterrorism Act of 1986 requires the Secretary of State to develop and implement security-related procedures and programs for U.S. Government foreign operations. Primary responsibility for the security of posts rests with the Chiefs of Mission under 1 FAM 013.2 and 2 FAM 113.1. Assistant Secretaries have the same responsibilities for domestic operations under provisions of 12 FAM 615.18. However, there is no requirement for Chiefs of Mission and Assistant Secretaries to notify DS or the Corporate Information System Security Officer when employees are designated Information System Security Officers or alternates. Consequently, DS cannot ensure the designees have sufficient training and experience to perform their Information System Security Officer responsibilities, which could result in unidentified minimum-essential cyber infrastructure vulnerabilities.

Recommendation 9: We recommend that the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to require that it be given the names of Information System Security Officers, and their alternates, in a timely manner, and that the Bureau of Diplomatic Security ensure all designees have sufficient experience and training.

Comments by the Bureau of Diplomatic Security: The Bureau commented that 12 Foreign Affairs Manual 600 will be amended to require that written notification of appointments or changes be sent to the Bureau, and that the Bureau will provide the information to other pertinent offices.

Comments by the Bureau of Information Resource Management: The Bureau of Information Resource Management suggested we revise Recommendation 9 to include the Corporate Information Systems Security Officer. The Bureau of Diplomatic Security has committed to providing the information to all other pertinent offices. We believe that having a single point of contact for this reporting will cause less confusion among Information Systems Security Officers here and abroad.

## Minimum-Essential Cyber Infrastructure Security Awareness and Training

Information technology security awareness and training can reduce exposure to known risks, but only if all employees are appropriately educated about the security of minimum-essential cyber infrastructure. The Department does not have sufficient policies, procedures, and programs to assure that employees are trained to properly secure the Department's information systems in general and its minimum-essential cyber infrastructure in particular.

The Computer Security Act of 1987 requires mandatory periodic security awareness and training in accepted security practices for everyone involved in managing, using, or operating sensitive cyber systems. The training is required to enhance awareness of cyber vulnerabilities and threats, and encourage improved security practices. The procedures, scope, and manner of the security awareness and training must comply with National Institute of Standards and Technology (NIST) and U.S. Office of Personnel Management (OPM) guidance. (See Appendix C for the requirements.)

OPM requires information technology security training for new employees within 60 days of hiring.[19] OPM also requires that all employees receive the training when they enter new positions dealing with sensitive information, or when their information security environment or procedures change significantly. OPM also requires periodic refresher training.

The Under Secretary for Management's directive, Security of Automated Information Systems, mandates establishing security education and awareness programs to inform managers and employees of their responsibilities. DS is responsible for administering the Department's information systems security training and awareness program, including minimum-essential cyber infrastructure. The Under Secretary's directive has criteria for measuring compliance with the security standards and states that assistant secretaries will be held accountable for adhering to published security standards.

In October 2000, the Secretary of State sent a cable to all posts requiring that proper handling and safeguarding of classified material and information be included in the work requirements statements and employee evaluation reports of all Foreign Service employees and supervisors. The Director General of the Foreign Service and Director of Human Resources (DGHR) are developing similar requirements for Civil Service employees and supervisors, which will become effective starting with the 2001 performance plans.

Currently, only computer operations staff and applications managers are accountable for information system security under 12 FAM 600. However, 12 FAM 600 does not reference the new Department policies requiring that supervisors use performance requirements and appraisal processes to hold employees accountable for meeting the Department's information security standards, including those that relate to minimum-essential cyber infrastructure.

Although the 12 FAM 600 appendix identifies the Computer Security Act of 1987, and the NIST, OPM, and National Security Telecommunications and Information Systems Security Committee

[19] Source: 5 CFR Part 930, Subpart C, Employees Responsible for the Management or Use of Federal Computer Systems.

(NSTISSC) awareness and training requirements, it does not describe how the Department will implement those requirements. Specifically:

- 12 FAM 600 does not reference the OPM requirement that all personnel with access to the Department's information systems are to have site-specific information technology systems security training related to their responsibilities for the systems within 60 days of their being granted access to the systems;
- 12 FAM 600 does not require periodic and threat-specific continuing or refresher cyber security training as required by the Computer Security Act of 1987;
- 12 FAM 600 does not require certification that all personnel having access to the Department's systems have received applicable initial and continuing systems security awareness and training, even for minimum-essential cyber infrastructure, as required by OMB Circular No. A-130, Appendix III; and
- 12 FAM 600 excludes contractors and the personnel of other agencies who have access to the Department's information systems from the mandatory refresher briefings conducted annually as required by OMB Circular No. A-130, Appendix III.

Enhanced procedures would require bureaus and offices to certify to the CIO that all constituent units fully comply with applicable requirements and have documentation supporting the certifications. The units could use existing documentation to support the certifications that they meet all applicable awareness and training requirements. Such documentation includes the Password Receipt and Security Acknowledgement Form requiring users to certify they will comply with all applicable security standards that could also require systems managers to certify users have actually completed applicable security standards training.

Addressing the issues described above will enhance the Department's ability to fully comply with the cyber security awareness and training requirements of the Computer Security Act of 1987, and relevant provisions of NIST, OPM, and NSTISSC policies. This requires developing and implementing better-organized approaches to ensuring all employees receive the awareness and training required by Federal laws, policies, regulations, programs, and procedures.

Recommendation 10: We recommend the Director General of the Foreign Service and Director of Human Resources submit language to the Bureau of Diplomatic Security amending 12 Foreign Affairs Manual 600 to require that all job and work requirements statements include individual responsibilities for minimum-essential cyber infrastructure security.

Recommendation 11: We recommend that the Director General of the Foreign Service and Director of Human Resources submit language to the Bureau of Diplomatic Security amending 12 Foreign Affairs Manual 600 to require that all supervisors assess the extent to which all employees accomplish their individual roles and responsibilities for minimum-essential cyber infrastructure security.

Comments by the Director General of the Foreign Service and Director of Human Resources on Recommendations 10 and 11: The Director General of the Foreign Service and Director of Human Resources stated that the Security Awareness and Accountability message contained in his ALDAC (State 203676, October 21, 2000) addresses the concerns found in Recommendations 10 and 11. Although the ALDAC does address the handling of classified documents and information by Foreign Service employees, it does not specifically address the responsibilities of all Department employees for minimum-essential cyber infrastructure security.

The Director General also commented that the Bureau of Diplomatic Security is responsible for the 12 Foreign Affairs Manual. Therefore, we changed the wording of Recommendations 10 and 11 to recommend the Director General submit appropriate language to the Bureau of Diplomatic Security to amend 12 Foreign Affairs Manual.

Recommendation 12: We recommend that the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to specify how the Department will implement the Computer Security Act of 1987, National Institute of Standards and Technology, U.S. Office of Personnel Management, and National Security Telecommunications and Information Systems Security Committee requirements for individual and organizational cyber security awareness, training, and accountability involving minimum-essential automated information infrastructure security.

Comments by the Bureau of Diplomatic Security: The Bureau commented that the authorities noted by the OIG are currently referenced in 12 Foreign Affairs Manual 600 We agree the authorities cited in Recommendation 12 are named in the manual, but neither the manual nor any other document of which we are aware specifies how the Department will implement those requirements of the authorities for individual and organizational cyber security awareness, training, and accountability involving minimum-essential cyber infrastructure security.

Recommendation 13: We recommend that the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to require that users be informed of, and acknowledge, their automated information security responsibilities prior to being granted access to Department systems.

Comments by the Bureau of Diplomatic Security: The Bureau concurred that 12 Foreign Affairs Manual 600 should address the Department's need to protect itself by requiring users to acknowledge their responsibilities prior to accessing its systems. The Bureau said the requirement would be included in a future revision of the Manual.

Recommendation 14: We recommend the Bureau of Diplomatic Security publish criteria for role- and access-based automated information systems security training, and for testing users for minimum levels of understanding of the automated information systems security criteria that apply to their roles and access levels. These Automated Information Systems Security Training Guidelines should comply with 5 Code of Federal Regulations Part 930, Subpart C, National Institute of Standards and Technology Special Publication 800-16, National Security Telecommunications and Information Systems Security Committee, and other applicable Federal Government directives and standards.

Comments by the Bureau of Diplomatic Security: The Bureau concurred with Recommendation 14.

Recommendation 15: We recommend the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to require that users demonstrate adequate understanding of their automated information systems security responsibilities, based on the Department's Automated Information Systems Security Training Guidelines, within 30 days of being granted access to systems, and at least annually thereafter. This recommendation is based on the assumption that the Bureau will complete the Guidelines as it has agreed to do in Recommendation 14.

Comments by the Bureau of Diplomatic Security: The Bureau agreed with Recommendation 15.

Comments by the Bureau of Information Resource Management: The CIO suggested we consider removing this recommendation unless we are more specific about how users would demonstrate adequate understanding of their responsibilities. As there is more than one way to achieve the recommendation, we believe the Bureau of Diplomatic Security should make this decision based on its assessment of the available choices.

Recommendation 16: We recommend that the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to require that users receive periodic and threat-specific continuing and refresher security training for automated information systems.[20]

Comments by the Bureau of Diplomatic Security: The Bureau agreed with Recommendation 16, and stated that 12 Foreign Affairs Manual 600 will be amended to require that users receive periodic and threat-specific continuing and refresher security training for automated information systems.

---

[20] Although providing user security awareness training at posts is the responsibility of the Information System Security Officer, general security awareness training is the responsibility of the Regional or Post Security Officers. However, with the agreement of their Information System and Regional Security Officers, posts may elect to incorporate user awareness training into general personnel security briefings.

Recommendation 17: We recommend the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to require executive or principal officers of all posts, bureaus, and offices to annually certify to the Chief Information Officer and the Bureau of Diplomatic Security their compliance with the Department's Automated Information Systems Security Training Guidelines developed by the Bureau of Diplomatic Security.

Comments by the Bureau of Diplomatic Security: The Bureau agreed with Recommendation 17 on the basis that certification can be a means of ensuring that documentation of user briefings is accurately maintained at posts and other offices. Cyber security assessments conducted by the Bureau and the OIG will measure the level of compliance. The Bureau also noted the posts could use this process to identify training deficiencies and assist the Bureau in establishing priorities for its training resources.

# List of Recommendations

Recommendation 1: We recommend the Assistant Secretary for International Narcotics and Law Enforcement Affairs, acting as the Foreign Affairs Functional Coordinator, seek to have the National Security Council Policy Coordination Committee on Counter-Terrorism and National Preparedness, which incorporates the Subgroup on International Cooperation of the NSC Critical Infrastructure Coordination Group, expand its approach to international critical infrastructure protection. This approach should include:

- coordinating the efforts of U.S. Government sector leaders to provide critical infrastructure protection information and assistance to a wide range of friendly countries requesting such assistance,
- focusing the efforts of U.S. Government sector leaders, Department missions, trade and business groups, and international organizations on actively promoting critical infrastructure protection preventative measures,
- encouraging multilateral cooperation, contingency planning, and open exchange of public information with the widest possible range of friendly countries and international organizations,
- supporting Department of State posts in engaging foreign governments in joint efforts to prevent or otherwise solve critical infrastructure protection problems, and
- using the expertise and resources of the International Information Programs Coordinator in developing and implementing the Working Group's outreach efforts.

Recommendation 2: We recommend the Assistant Secretary for International Narcotics and Law Enforcement Affairs, acting as the Foreign Affairs Functional Coordinator, work with U.S. Government and nongovernmental organizations to provide friendly foreign governments with opportunities for obtaining cyber law enforcement training and technical assistance.

Recommendation 3: We recommend the Assistant Secretary for International Narcotics and Law Enforcement Affairs, acting as the Foreign Affairs Functional Coordinator, work with the Department of Justice to identify and disseminate through posts more efficient and effective communications channels for processing foreign governments investigative assistance requests, and improved procedures for gaining more timely access to evidence, that foreign law enforcement entities can use to enhance their investigations of cyber crimes involving United States entities and individuals.

Recommendation 4: We recommend the Chief Information Officer and the Assistant Secretary for Diplomatic Security address the Department's foreign operations in subsequent critical infrastructure protection plans and vulnerability assessments to determine what, if any, overseas minimum-essential cyber infrastructure should be subject to vulnerability assessments. In doing so, Department officials should include representatives of other agencies having an overseas presence in developing the overseas portion of the plans, and conducting and assessing the overseas portion of the vulnerability assessments as appropriate.

Recommendation 5: We recommend the Bureau of Diplomatic Security schedule and conduct security controls evaluations of all minimum-essential cyber infrastructures at least once every 3 years, and whenever there are significant changes to minimum-essential cyber infrastructure, both as required by OMB Circular No. A-130, Appendix III.

Recommendation 6: We recommend the Bureau of Diplomatic Security modify 12 Foreign Affairs Manual 600, and the Bureau of Information Resource Management amend the Critical Infrastructure Protection Plan, to require periodic security control evaluations of all minimum-essential cyber infrastructure at least once every 3 years.

Recommendation 7: We recommend the Chief Information Officer and Bureau of Diplomatic Security ensure that subsequent critical infrastructure protection plans and vulnerability assessments address minimum-essential interagency infrastructure vulnerabilities.

Recommendation 8: We recommend the Assistant Secretary for Diplomatic Security, Chief Information Officer, and the Director of the Foreign Service Institute jointly develop and implement interagency critical infrastructure protection practices and procedures training and exercises that meets the requirements of Presidential Decision Directive 63.

Recommendation 9: We recommend that the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to require that it be given the names of Information System Security Officers, and their alternates, in a timely manner, and that the Bureau of Diplomatic Security ensure all designees have sufficient experience and training.

Recommendation 10: We recommend the Director General of the Foreign Service and Director of Human Resources submit language to the Bureau of Diplomatic Security amending 12 Foreign Affairs Manual 600 to require that all job and work requirements statements include individual responsibilities for minimum-essential cyber infrastructure security.

Recommendation 11: We recommend that the Director General of the Foreign Service and Director of Human Resources submit language to the Bureau of Diplomatic Security amending 12 Foreign Affairs Manual 600 to require that all supervisors assess the extent to which all employees accomplish their individual roles and responsibilities for minimum-essential cyber infrastructure security.

Recommendation 12: We recommend that the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to specify how the Department will implement the Computer Security Act of 1987, National Institute of Standards and Technology, U.S. Office of Personnel Management, and National Security Telecommunications and Information Systems Security Committee requirements for individual and organizational cyber security awareness, training, and accountability involving minimum-essential automated information infrastructure security.

Recommendation 13: We recommend that the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to require that users be informed of, and acknowledge, their automated information security responsibilities prior to being granted access to Department systems.

Recommendation 14: We recommend the Bureau of Diplomatic Security publish criteria for role- and access-based automated information systems security training, and for testing users for minimum levels of understanding of the automated information systems security criteria that apply to their roles and access levels. These Automated Information Systems Security Training Guidelines should comply with 5 Code of Federal Regulations Part 930, Subpart C, National Institute of Standards and Technology Special Publication 800-16, National Security Telecommunications and Information Systems Security Committee, and other applicable Federal Government directives and standards.

Recommendation 15: We recommend the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to require that users demonstrate adequate understanding of their automated information systems security responsibilities, based on the Department's Automated Information Systems Security Training Guidelines, within 30 days of being granted access to systems, and at least annually thereafter. This recommendation is based on the assumption that the Bureau will complete the Guidelines as it has agreed to do in Recommendation 14.

Recommendation 16: We recommend that the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to require that users receive periodic and threat-specific continuing and refresher security training for automated information systems.

Recommendation 17: We recommend the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to require executive or principal officers of all posts, bureaus, and offices to annually certify to the Chief Information Officer and the Bureau of Diplomatic Security their compliance with the Department's Automated Information Systems Security Training Guidelines developed by the Bureau of Diplomatic Security.

# Abbreviations

| | |
|---|---|
| CIO | Chief Information Officer |
| CIP | Critical Infrastructure Protection |
| CIPP | Critical Infrastructure Protection Plan |
| Department | Department of State |
| DGHR | Director General of the Foreign Service and Director of Human Resources |
| DS | Bureau of Diplomatic Security |
| FAM | Foreign Affairs Manual |
| INL | International Narcotics and Law Enforcement Affairs |
| IRM | Bureau of Information Resource Management |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| OPM | U.S. Office of Personnel Management |
| NSC | National Security Council |
| NIST | National Institute of Standards and Technology |
| NSTISSC | National Security Telecommunications and Information Systems Security Committee |
| NTISSD | National Telecommunications and Information Systems Security Directive |
| NSTISSI | National Security Telecommunications and Information Systems Security Instructions |
| PDD | Presidential Decision Directive |