MEMORANDUM REPORT NUMBER IT-A-02-01

CLASSIFIED CONNECTIVITY PROGRAM:

PROGRESS AND CHALLENGES

February 2002

The Classified Connectivity Program (CCP) is an ongoing effort within the Department to deploy a standards-based, global network for classified information processing and communications to about 250 embassies and consulates overseas. The program is intended to assist the Department in meeting objectives in its Information Technology (IT) Strategic Plan, FY 2001-FY 2005, of supporting its international affairs and diplomatic mission with modern, robust, secure, and cost-effective IT solutions.

This report focuses on the Department's strategy for implementing the CCP to modernize classified local area networks (C-LANs) at its overseas posts. Specific objectives of our review were to: (1) determine what, if any, security or operational problems are inherent in current C-LANs overseas; (2) assess the Department's approach to planning and implementing its C-LAN systems modernization via the Classified Connectivity Program; and (3) identify what changes may be needed to the Department's modernization initiative. The purpose, scope, and methodology for our review can be found at Appendix A.

RESULTS IN BRIEF

Since 1998, the Department has had an ongoing effort to institute up-to-date C-LAN equipment to help carry out the U.S. foreign affairs mission at about 250 of its diplomatic and consular posts.[1] The overwhelming majority of overseas posts have had no classified connectivity or inadequate support from outdated networks, which are increasingly difficult to maintain. The Department's initial approach to C-LAN modernization, however, was largely unstructured and with limited funding made minimal progress—completing only about 20 installations in 1998-99 in contrast to its original objective of 48 deployments per year over a 5-year period. The Secretary has made instituting up-to-date technology to support classified communications a high priority within the Department, spurring efforts to complete CCP deployments

[1] Some posts do not meet the requirements for classified processing and will not receive the modernized C-LAN equipment.

to all eligible posts by December 2003. Under the direction of the Program Management and Analysis (PMA) Division within the Bureau of Information Resource Management (IRM), the Department now has a disciplined CCP approach in place and is making continued progress toward meeting this priority objective. Since assuming responsibility for the project, PMA has completed an additional 55 deployments, for a total of 75 C-LAN modernizations as of September 2001.

Despite the Secretary's priority emphasis, CCP implementation efforts have had a history of funding uncertainties that have challenged PMA's ability to accomplish the project on schedule. Though program funding is currently back on track, CCP implementation remains challenged by issues with equipment procurements, deployment logistics, and delays in bandwidth installations that also pose potential risks for the program schedule. The current project approach does not include a documented strategy for CCP certification and accreditation to help identify and manage systems security risks. Further, C-LAN deployments are not adequately supported by IT contingency plans to ensure business continuity in case of failures, disruptions, or emergencies that affect systems operations at overseas posts.

Provision of adequate and timely funding will help keep this priority program on schedule through its completion. The Department can also improve program planning to ensure that systems certification and accreditation are conducted, risks are effectively managed, and effective IT contingency strategies are in place to help safeguard classified information processing overseas. Such precautions are especially critical in the current environment of increasing systems security threats and in view of IT deficiencies we identified in recent OIG inspection reports and an assessment mandated by the Government Information Security Reform Act (GISRA).[2]

BACKGROUND

Since 1998, IRM has been working to institute a worldwide IT infrastructure to support routine and crisis processing of classified information. This program, formerly known as C-NT LAN[3] modernization, was restructured in October 1999 as the CCP within PMA. The CCP is the classified counterpart to A Logical Modernization Approach (ALMA), the recently completed project to install new servers and

[2] *Senior Management Attention Needed to Ensure Effective Implementation of the Government Information Security Reform Act*, OIG Memorandum Report Number 01-IT-M-082, September 2001.

[3] The "NT" in the acronym refers to the Windows New Technology (NT) operating system on which the modernized C-LAN systems are based.

desktop computers for sensitive but unclassified processing at overseas missions. The CCP addresses the lack of classified connectivity at many posts, along with problems in other locations with existing Banyan local area networks that are based on older proprietary hardware and software and require inefficient user processes. The Banyan networks are also subject to extended outages and are increasingly difficult and costly to maintain. Replacement of the outdated classified client server infrastructure is not an option because Banyan is no longer supported by the designated supplier.

The entire C-LAN modernization effort involves installation of new classified networks at approximately 250 overseas locations by the end of 2003, at a total program cost of about $200 million. Of the approximately 250 locations, C-LAN equipment is being replaced at about 100 posts that have outdated Banyan or Classified Information Handling System equipment.[4] Classified connectivity is also being provided to 145 overseas missions that have had no classified systems or e-mail at all. Locations without classified connectivity have had to rely on other means, such as secure telephone, fax, and pouch mail, to conduct classified operations—an untenable situation in the current information age. Many of these missions are located in politically sensitive and high-threat regions where rapid and secure communications are especially critical to ensure the security of American citizens abroad during a crisis.

Like ALMA, the CCP is implementing commercial off-the-shelf technology—specifically, Windows NT operating systems and new hardware, software applications, and networks—for classified processing and communications worldwide up to the secret level. The program is eliminating the need for the redundant gateways, technical support, and systems administrator training now in place just for the Banyan systems. Standard equipment deployments are intended to minimize the need for posts independently to implement a variety of incompatible systems—a situation that has become increasingly problematic. New or expanded capabilities supported by the classified program include office automation products, e-mail, browsing technology, and advanced firewall security and encryption technology. The program also includes faster telegraphic communications via CableXpress, a system for electronic cable distribution at the desktop. CCP facilitates centralized and regionalized storage of classified information, as well as selected data sharing among overseas missions and Federal agencies via the Secret Internet Protocol Router Network (SIPRNET), a program that uses classified Internet browsing technology.

[4] The Classified Information Handling System is hardware and software previously used within the Department for encrypting and transmitting classified telegrams over unclassified circuits.

REVIEW FINDINGS

IMPROVED APPROACH TO CCP IMPLEMENTATION

The Department has made several enhancements to its strategy for modernizing its C-LAN systems overseas. Institution of more disciplined practices, partnering with the functional and geographic bureaus, and adoption of more efficient processes are some of the key improvements identified in the project management approach.

Initial Approach to CCP Was Unstructured

From 1998 through 1999, IRM's Messaging Systems Office, in partnership with the Office of Information Technology Infrastructure, LAN and WAN Services Division, managed the original CCP. The primary objective of the program at that time was to replace outdated Banyan classified networks at a rate of 48 overseas posts per year. IRM conducted surveys of overseas posts, purchased and installed equipment, and provided training. Theirs was largely an unstructured approach, with no established procedures, templates, or project management checklists. As a result, the entire process for a single C-LAN installation required as much as 3 to 7 months for completion. Given this, along with staffing and funding limitations, IRM deployed modern classified networks to a total of 20 locations overseas during the first 2 years of the program.

More Disciplined Program Management Approach

In October 1999, IRM's Program Management and Analysis (PMA) Division assumed management responsibility for the C-LAN modernization effort. Established as an offshoot of the ALMA program, PMA is currently responsible for large-scale deployment of the Department's worldwide Information Technology Infrastructure. Currently, PMA is managing two other programs—ALMA Refresh, and Public Diplomacy "Almatization"—in addition to the classified network modernization program. In total, PMA manages about $47 million worth of IRM programs, all funded primarily from the Central Investment Fund.

Within 3 months of assuming C-LAN modernization responsibility, PMA reengineered the program, renaming it the CCP. PMA instilled discipline by applying generally accepted project management practices and required methodologies, such as Managing State Projects, to the CCP. CCP implementation has been a complex undertaking involving the following activities:

- Conducting initial e-mail surveys of over 200 posts to determine basic customer business requirements, followed by physical survey of each site to identify specific IT infrastructure requirements;

- Developing 10 core configuration templates and corresponding cost models for C-LAN installations at overseas posts;

- Conducting market surveys to establish vendor and technical criteria, identify potential vendor sources, and encourage competition among suppliers of commercial off-the-shelf, Tempest, and zoned equipment;

- Obtaining formal design acceptance from posts and initiating equipment procurements to meet post configuration requirements;

- Ensuring security planning and coordinating infrastructure and network support with relevant Department organizations;

- Receiving, testing, integrating, and preparing computing equipment for classified pouch shipment overseas; and

- Coordinating schedules and deploying teams to install C-LAN equipment at each target location.

CCP also involves coordination among many different activities and organizations. Including the regional bureaus in the project management decisionmaking process was one of the most constructive changes made to the program. Recognizing that the regional bureaus would benefit most from a deployment plan that considers the various criteria of individual posts (i.e., political sensitivities, available bandwidth, and IT and host nation infrastructure) PMA joined with the regional bureaus to develop a process whereby the bureaus prioritized overseas posts for C-LAN installations. PMA works to keep the bureaus involved and up-to-date on the C-LAN installation progress. At times, PMA coordinates with regional bureaus and posts willing to provide funding of their own to help further C-LAN installations. For example, in FY 2000, the Bureau of European Affairs provided funding to the CCP for modernizations at 16 posts. At least three other embassies funded C-LAN installations to support their own operations or those of nearby consulates.

Further, PMA has established service level agreements to govern other cooperative arrangements. For example, an agreement with IRM's LAN and WAN Services Division outlines this organization's responsibility for conducting and documenting site surveys, preparing approved design packages, performing installations, designing formal architectural drawings, and coordinating installation activities with posts. PMA also signed service level agreements with the Foreign Service Institute's School of Applied Information Technology to secure systems administrator and end-user training on the CableXpress application. Additionally, PMA holds periodic meetings with key organizational representatives to discuss cross-functional program issues, address infrastructure and network support issues, coordinate ongoing operations, and develop processes and policies for achieving program goals and objectives.

Throughout the CCP effort, PMA has sought to improve its project management approach, incorporating a number of innovations. For example, PMA applied lessons learned from life-cycle management of the ALMA program. The division developed technical and financial databases of systems information for nearly all of the Department's overseas sites. The financial database serves as a management information system for controlling the resources associated with the various IT modernization initiatives under PMA management. The technical database basically documents systems design. As such, it establishes a baseline to control systems configurations, guide systems upgrades, and support future systems implementations. The technical database serves as a web-based resource that program managers, technical personnel, and post officials can all access.

Further, PMA encouraged a competitive contracting environment, consolidated equipment and materiel requirements, and reduced the number of shipments, thereby producing real savings for each core system in comparison to C-LAN modernization costs under prior program management. In addition, PMA worked with acquisition officials to streamline the procurement process, including requesting quotes for equipment early in the planning process and purchasing the equipment as funding is released instead of waiting until they receive full funding. Further, PMA established a new facility to improve warehousing, integrating, and preparing C-LAN equipment for shipment.

Challenges to Successful CCP Implementation

The CCP is one of the Department's top three priority IT initiatives. Though currently back on track, the CCP has had a history of funding uncertainties that have challenged its successful implementation. The program has also met with a number of funding, logistical, and procurement challenges that have a direct impact on project implementation schedules. If not successfully overcome, such challenges could hinder project managers' ability to complete C-LAN installations at all eligible posts by the December 2003 deadline.

Funding Delays Challenged the CCP Implementation Schedule

Adequate and timely funding has been a problem throughout the history of the CCP. Repeatedly the program has met with shortages or delays in funding that have hindered implementation. The following is a summary of CCP funding since the program's inception:

- FY 1998-99: The Department spent approximately $10.2 million on start-up activities and installation of new classified equipment at the first 20 locations. Much of this initial effort was done to replace legacy and outdated systems at a number of posts to help ensure that computers would continue to function properly after the January 1, 2000, date change. Apart from Year 2000 remediation efforts, the majority of the Department's IT funding was devoted to operations and maintenance activities rather than to modernization initiatives.

- FY 2000: Around the time that PMA assumed responsibility for the program, funding had diminished to $1.6 million carried over from the prior year and previous program management. By January 2000, PMA was forced to cut back on C-LAN modernization activities and terminate about 25 contract personnel. As a result, PMA completed only 3 CCP installations and limited work in many instances to establishing dial-up classified access for only those posts with no C-LAN capability at all. PMA ultimately received about $3.2 million in central investment funds to help sustain the program.

- FY 2001: Again, the program received $3.2 million from the central investment fund, and an additional $5 million via the financial plan developed through the Department's internal process for making budget allocation decisions.

The Secretary's call for modernization of the Department's IT systems to support diplomacy in the current information age has become the driving force for completing the CCP within the next 2 years. This priority was outlined in the President's Budget for FY 2002, presented in February 2001. However, midyear funding presented a significant impediment to CCP progress in meeting this objective. Midyear funding refers to the delays experienced in receiving program funds as the Department works through its internal routine process of allocating funds from Congressional appropriations, which may not have been enacted until well into the fiscal year. Specifically, in early April 2001, PMA formally requested funds from IRM, FMP, and Bureau of Administration managers in the amount of $8.7 million by mid-April and $16.3 million by early July 2001. PMA officials stated that the amounts and the timing specified for funding were necessary to "kick start" phase two of the CCP to meet their ambitious 2-year installation schedule. However, PMA did not receive the approximately $26 million in requested funding until the mid-June to July 2001 time period, requiring that the division compress the program schedule to compensate for the funding date change.

According to PMA officials, when they do not get the funds needed on time and in the amounts specified, planning for this complex program "falls apart." Specifically, the 2-month funding delay meant redoing plans and postponing critical CCP activities, such as site surveys and corresponding development of approved design packages for post installations. Procurement of Tempest and zoned equipment that already typically requires lead times of 90 to 120 days were pushed further out.[5] Readiness of the new facility acquired for warehousing, integrating, and packing and crating of C-LAN equipment in preparation for shipment was also slowed.

As of September 2001, CCP funding was on track given receipt of the $26 million in funding during the preceding summer. Despite prior years' budget uncertainties, the funding outlook for the CCP in FY 2002 appears positive. By conference agreement on November 9, 2001, the Congress appropriated funds for Department programs. The agreement specifies approximately $107 million for the replacement of computer and communications equipment that posts use for classified operations. The Department is now preparing a financial plan, which it will use to allocate funds in accordance with Congressional direction. The Under Secretary for Management will have responsibility for the final IT funding decisions based on recommendations of other senior managers in the Department.

[5] Tempest equipment is technology that has been designed or modified to suppress compromising signals and has been approved at the national level for U.S. classified information processing after undergoing specific tests. Zoning refers to the selection and placement of classified equipment within predetermined secure areas of a facility in order to contain radiated emanations.

Ongoing Risks to CCP Implementation Schedule

CCP progress is faced with various other risks, for which PMA has taken considerable countermeasures but has no definitive solutions. Specifically, as stated in monthly status reports to the Under Secretary for Management since June 2001, CCP progress could potentially be deterred by risks in the following areas:

- Procurement: Contract and procurement procedures are cumbersome and slow, and there are a limited number of vendors with limited capacity to meet the increased volume of equipment delivery orders.

- Logistics: Packing and crating operations are currently at peak capacity. It is not certain whether the current controlled pouch system will be able to accommodate an increase in surface shipments of 150,000 pounds per month, and pouch shipments by air are too expensive.

- Space, Facilities, and Resources: The physical movement of goods currently requires six moves. Cleared storage, integration, and office space is at capacity and additional resources are required to make the new warehouse operational.

- Hardware: Production has ceased on current, approved network encryption devices and the availability date remains unknown for successor devices.

- Bandwidth: As of September 2001, over 30 posts still had less than the minimum requirement of 64 kilobytes per second of bandwidth. The Diplomatic Telecommunications Service Program Office (DTS-PO) is responsible for providing bandwidth needed to support C-LAN installations.

PMA officials discussed with us their remediation strategies for countering these risks. For example, PMA officials have worked with acquisition officials to identify multiple sources of supply and increase competition among vendors. They have also included supplier ability to deliver equipment on schedule as a criterion for contract award decisions, thereby better ensuring prompt deliveries and reducing the lead time needed for equipment procurements. The new warehouse and integration facility constructed to facilitate logistics management was completed on time and is already in use.

PMA officials told us that they had also stockpiled about 72 of the current, approved encryption devices to support CCP deployments through June 2002 and anticipate that the successor devices will be available shortly thereafter. In August

2001, IRM submitted requests to DTS-PO for additional bandwidth to support both the CCP and the OpenNet Plus Program, which is intended to provide Internet access at the desktop for Department users at locations worldwide. Obtaining the minimum bandwidth needed for CCP is first priority. Posts for which providing bandwidth is most difficult will be last on the list to receive the modern C-LAN equipment, allowing added time for the bandwidth installations.

Further, PMA officials recognize their limitations to address risks regarding peak capacity packing and crating and shipping operations. Because they are not currently shipping, they do not know whether they will be able to meet increased deployment requirements. However, PMA officials said that they are planning ahead as much as possible and remain optimistic about meeting their ambitious CCP deployment schedule.

Current Status of CCP Installation Progress

Despite the challenges, the CCP effort continues to move forward. In addition to the 20 installations carried out under prior program management, PMA has completed 55 more installations, for a total of 75 C-LAN modernizations under CCP Phase I. This first phase of the program involves funding and activities from the program start in 1998 through about January 2002. CCP Phase II, scheduled to begin in mid-FY 2002, involves installing modern C-LAN at 180 additional posts and revisiting 10 other combination classified NT/Banyan LAN posts that require upgrades. Regional bureau priorities for installing C-LAN equipment at the first 50 posts scheduled under CCP Phase II are to be addressed starting in April 2002 and due to be completed by the end of FY 2002. C-LAN installations at the remainder of the approximately 250 candidate posts are due to be completed by December 2003. The total cost for CCP implementation is estimated at about $200 million, including approximately $50 million in infrastructure support costs for such items as network management and bandwidth augmentation.

CCP Security Planning Needs Improvement

The Department lacks a documented approach for managing the security risks of modernized C-LAN equipment being deployed to its overseas posts. The Department's IT contingency planning efforts also have not been adequate to help ensure that systems such as the new C-LAN are covered by strategies for continuing or restoring mission-critical operations in case of unexpected disruptions in service. Addressing these issues is essential, especially given general IT and C-LAN-specific security weaknesses OIG identified in various reports over the past 2 years.

No Definitive CCP Certification and Accreditation Strategy

The Department has not developed a definitive strategy for managing the security risks of its CCP deployments. As directed by various legislation and policy guidance,[6] executive departments and agencies are to establish processes for authorizing and ensuring the security of the IT systems that they implement. The National Information Assurance Certification and Accreditation Process (NIACAP) developed by the National Security Telecommunications and Information Systems Security Committee outlines a phased, risk-management framework for meeting these IT security requirements.[7] Specifically, the NIACAP outlines the minimum national standards, activities, general tasks, and management structure for systems certification and accreditation. The NIACAP defines certification as the independent, technical review of a system to identify risks and ensure that the system meets Federal IT security requirements. Accreditation is the subsequent formal acceptance of the risks identified through certification and approval to operate the system, ensuring that the accredited security posture will be maintained throughout the system life cycle. The NIACAP directs that a System Security Authorization Agreement (SSAA) be initiated at the outset of an IT project to guide certification and accreditation activities and document agreements among responsible authorities.

The Bureau of Diplomatic Security (DS)—the Department's certification authority—has not completed the steps needed to certify the classified Windows NT LAN in accordance with Federal requirements. In an April 1999 memorandum, DS approved IRM use of standard software to begin the CCP. DS provided the initial approval on the condition that all systems configurations and settings be performed as outlined in supporting documentation, and with the assumption that the required physical, personnel, and emanation security environments are established to support the system. Despite ongoing C-LAN deployments, DS has subsequently not worked to certify the system and ensure that these conditions and assumptions were fulfilled.

[6] *Computer Security Act of 1987(Public Law 100-235, as amended)*; Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, Appendix III; and The Federal Information Processing Standard Publication 102, *Guidelines for Computer Security Certification and Accreditation*.

[7] The four phases of the NIACAP are definition, verification, validation, and post accreditation.

In recent discussions, DS officials told us that, as authorized by the NIACAP, they plan to recommend a "type accreditation" of the CCP configuration. As defined in the NIACAP, a type accreditation evaluates an application or system that is distributed to a number of different locations. As such, DS officials believe that a type accreditation is appropriate for the CCP, which involves deploying a simple, standard, hardware and software configuration to multiple posts worldwide. DS officials stated that the type accreditation would be supported by a central SSAA, with input by the PMA and various other organizations, as a basis for a final accreditation decision.

Further, DS officials said that they would travel abroad to certify the C-LAN in each overseas post environment, starting in late FY 2003. They said that the C-LAN certifications overseas will be conducted in conjunction with certification and accreditation for the OpenNet Plus program. Both the CCP and the OpenNet Plus Program are based on standard hardware and software configurations using the same telecommunications infrastructure, with the only differences being bandwidth requirements and the classification levels of information. DS officials said that the joint certification approach will involve assessments of all aspects of individual post environments (i.e., physical, personnel, and technical) that could affect the security of their classified information processing activities. DS officials indicated that post officials, such as the information management officer, regional security officer, or information systems security officer, who will be responsible for managing the operational systems, will also be responsible for developing the SSAAs to support systems certification and accreditation. DS officials stated that they would provide toolkits for posts to use in developing their SSAAs.

This overall certification and accreditation strategy may prove viable. However, we are concerned about certain aspects of the stated approach, such as delaying the C-LAN certification activities until FY 2003. According to the NIACAP, certification and accreditation of a system should be started at the beginning of a system's life cycle. Though C-LAN deployments have been completed at 75 locations since 1998, DS has not worked to test, verify, and ultimately certify the security of the classified processing environments. Posts are responsible for management and routine reporting of classified information processing operations in accordance with existing internal Department guidance and DS routinely sends teams overseas to evaluate compliance. Lacking certification, however, there is no central oversight or in-depth assessments to identify technical or environmental security risks. Lacking accreditation, there is also no formal acceptance or accountability for managing those risks by site managers or chiefs of mission. In December 2001, DS officials said that, using existing resources, the type accreditation would likely be conducted in 2002. However, due to funding constraints, they said that post visits and certifications would probably not occur for at least another year and a half. DS officials said that they planned to include funds for post certification activities in their FY 2003 budget.

Further, we are concerned about the lack of an overall documented plan for carrying out the C-LAN certification approach. Discussions between OIG and responsible DS and IRM officials have yielded conflicting perspectives on how C-LAN certification and accreditation might be conducted. The only documented certification and accreditation plans we identified are for the OpenNet Plus project, outlining plans for testing and independent verification and validation of that system alone. The testing will be conducted as a prelude to certification and accreditation, at a cost of $30 million for DS and $7 million for IRM. In the absence of a clear, documented strategy, it is not certain what the certification and accreditation will include, how it will be conducted, and at what cost.

In late December 2001, DS officials told us that they were planning to hold their first meeting to outline a strategy that would include the CCP type accreditation as well as subsequent certification and accreditation for posts worldwide. They said that the strategy would include details on their planned certification and accreditation approach, ultimately for presentation to the designated approving authority. They expected to have a first draft of the strategy by March 2002. At the time of our meeting, DS officials had no plans to include IRM representatives in their discussions to develop the strategy. We believe that IRM's involvement will be essential since it is the organization responsible for accrediting the CCP based on DS' certification recommendation. If not involved, the DS strategy might not provide all of the elements needed as a basis for the accreditation decision.

Federal requirements for systems certification and accreditation are not new, dating back to Federal Information Processing Standard 102, *Guideline for Computer Security Certification and Accreditation,* disseminated in September 1983. Since then, the Department has restated several times its commitment to complying with certification and accreditation requirements. However, to date, the Department has undertaken certification and accreditation of only 5 percent of the 370 major automated systems that OIG identified in our report on implementation of GISRA. The Department recently released *Certification and Accreditation (C&A) Process,* Version 1.0, August 2001, outlining its overall program for certifying and accrediting its IT systems. The process document is based on Department and National directives, including the NIACAP and National Institute of Standards and Technology guidance. When finalized, the document should strengthen the foundation for developing a well-defined C-LAN certification and accreditation strategy within the Department.

IT Contingency Planning Inadequate to Support CCP Implementation

The Department's IT contingency planning efforts have not been adequate to help safeguard classified information systems and the critical business functions that they support in the event of unexpected disruptions at posts overseas. As defined by the National Institute of Standards and Technology, an IT contingency is an event—such as a power outage, hardware failure, fire, or storm—with the potential to disrupt computer operations and the critical mission and business functions that they support. Office of Management and Budget Circular A-130 requires that agencies establish contingency plans for all major systems to ensure their ability to recover and provide service sufficient to meet the minimal needs of system users in the event of unplanned disruptions. The Office of Management and Budget also requires that agencies periodically test their contingency plans to ensure viability. The National Information Assurance Certification and Accreditation Process further requires that IT contingency plans be in place to support systems certification.

IT contingency planning involves the coordination of personnel and integration of a series of tasks, procedures, and information to direct actions for reducing confusion, improving communications, and achieving the timely continuation or resumption of business at the time of a disruption. IT contingency management strategies include a range of backup operations, remote data storage, communications rerouting, or alternate information processing capabilities. In accordance with foreign affairs guidance,[8] contingency plans are to be coordinated with Emergency Action Plans, which embassies and consulates are required to have for emergencies of any kind. Along with other requirements, IT contingency plans are also a critical element of the SSAA documentation required to support the systems certification and accreditation process.

Given the classified nature of the information processed on the system, IT contingency planning should be critical to supporting CCP deployment. However, OIG found that the Department has not given sufficient focus and emphasis to this activity. Based on various OIG and DS information security evaluations at overseas posts in recent years, a significant number of posts do not have IT contingency plans in place. IRM officials that we met with estimated that as many as 85 to 90 percent

[8] Department of State Foreign Affairs Manual 12, section 622.3-2.

of posts lack such plans. We found this to be the case despite the recent emphasis on contingency planning to support the Year 2000 date change less than 2 years ago. Further, there are currently multiple mechanisms in place for developing and implementing IT contingency plans. For example, we identified at least three toolkits or programs available to support IT contingency planning, as follows.

- The Diplomatic Security Training Center provides training for technical personnel on the development of Network Countermeasures Contingency Plans.
- A contingency guide developed by IRM's Office of Architecture, Planning, and Regulations is intended to help create cost-effective strategies for dealing with unexpected events.
- IRM's Systems Integrity Division is developing and testing tools for domestic organizations and overseas posts to implement IT contingency plans. IRM officials recently indicated that these tools will be used to support IT contingency planning as a prerequisite for obtaining OpenNet Plus capability.

The IT contingency planning programs that we identified emphasize different aspects of IT contingency planning. For example, the DS program focuses more on managing contingency events, while the IRM program emphasizes development of an inventory and database to help restore systems operations after a disruption. We nonetheless found that these plans have redundant requirements for meeting the same objectives, indicating a lack of oversight and coordination throughout the Department. Consolidation and integration of these programs would be appropriate for consistent IT contingency planning at headquarters, as well as at embassies and consulates abroad. This will be key to supporting not just the CCP, but systems security management in general within the Department's overall IT infrastructure.

Need for Improved CCP Security Planning Underscored in Recent Reports

Addressing these CCP security issues is essential, especially given increasing risks to information processing in the current technology age. Rapid expansion in computer interconnectivity poses significant risk of malicious intrusions into inadequately protected systems. Heightened dependence on automation to process sensitive information and conduct mission-critical business also enhances the need to control management and ensure proper use and functioning of computer networks hosted in U.S. missions abroad.

The need for effective CCP risk management strategies is underscored by recent OIG reports on a range of deficiencies in the Department's information security management environment. Specifically, our recent report on the Department's progress in implementing key requirements of GISRA[9] discussed broad deficiencies in information assurance. Both OIG and DS evaluations over the past 2 years identified weak information security management practices at dozens of overseas posts. OIG indicated, for example, that only 10 of the 35 posts in one region reviewed by OIG security teams in 1999 and 2000 had adequate information security procedures in place. According to OIG's survey questionnaire, although 59 percent of the Department's 371 systems are reported to have risk assessments, only 10 percent are reported to have security plans, as required by GISRA. OIG identified additional concerns with the Department's progress in developing and implementing its cyber-based critical infrastructure protection plan, as mandated by Presidential Decision Directive 63. According to DS officials, many of the reported information security issues are systemic and require a change in culture of the Department's systems management and users in order to be resolved.

Further, several OIG inspection reports in recent months identified C-LAN-specific management deficiencies in both the outdated Banyan and newly modernized C-NT LAN environments. These deficiencies include a lack of configuration management, access controls, and IT contingency planning, as discussed above. DS evaluations of classified operations at posts also identified deficiencies with C-NT LAN equipment. As part of our review, we studied a random sample of 21 DS reports from IT evaluations in the past 2-3 years and found instances where C-LAN servers had been locking up and showed signs of imminent system failure. The DS evaluation reports identified locations where C-LAN equipment without back-up programs also had the potential for network failures. DS evaluations we reviewed found that sometimes C-LAN users were not establishing passwords correctly to guard access to their workstations. The evaluations included discussions of embassies that did not have security settings for the C-LAN in accordance with the Department's Windows NT configuration standards. When done correctly, these settings help safeguard the integrity of information on the system from risk of compromise. Further, DS found a virus on one embassy's classified system. These are all issues that could be addressed through improved information security planning and risk management strategies as C-LAN modernization continues.

[9] *Senior Management Attention Needed to Ensure Effective Implementation of the Government Information Security Reform Act*, Office of Inspector General, U.S. Department of State, Memorandum Report 01-IT-M-082, September 2001.

Recommendation 1: The Bureaus for Information Resource Management and Diplomatic Security should develop a documented strategy and schedule for C-LAN certification and accreditation to help identify and manage risks to secure classified processing at overseas posts.

Recommendation 2: The Bureau of Information Resource Management should coordinate and consolidate its information technology contingency planning training and support activities with similar activities in other Department organizations to ensure that standardized approaches are used to develop and implement plans for safeguarding modernized classified processing operations in case of unexpected disruptions at overseas posts.

DEPARTMENT COMMENTS AND OUR EVALUATION

We obtained comments on a draft of this report from the Office of the Under Secretary for Management and the Bureaus of Information Resource Management and Diplomatic Security. We have incorporated their comments where appropriate and included copies of their comments at Appendix B.

In its comments, the Office of the Under Secretary for Management stated that it believed that a recommendation included in the draft report, which advised the office to ensure timely funding to help address identified risks and complete overseas C-LAN modernizations by the December 2003 deadline, was inappropriate. The office stated that connectivity, both classified and unclassified, is already the Secretary's highest IT priority and that instructions to implement the CCP are clear, requiring no recommendation from OIG in this regard. We deleted the recommendation from the report because, in contrast to prior years' uncertainties, the CCP funding outlook now appears more positive. By conference agreement on November 9, 2001, the Congress appropriated funds for Department programs, specifying approximately $107 million for the replacement of computer and communications equipment that posts use for classified operations. The Department is now preparing a financial plan, which it will use to allocate funds in accordance with Congressional direction. The Under Secretary for Management will have responsibility for the final IT funding decisions based on recommendations of other senior managers in the Department.

IRM and DS responses to Recommendation 1, directed to both their bureaus, do not adequately address our concerns about the approach to managing CCP information security risks. Specifically, IRM officials agreed with the recommendation, stating that IRM and DS have already developed preliminary strategies related to C-LAN certification and accreditation and have outlined an approach for joint implementation with the OpenNet Plus program. DS officials indicated that the Department has an established program for certification and accreditation of its classified and unclassified IT systems in compliance with Department and national directives. Further, DS officials discussed their commitment to independent verification and validation of the OpenNet Plus implementation project, which they believe will support the Department's certification and accreditation process scheduled to begin FY 2003.

We acknowledge the Department's development of a certification and accreditation process and its preliminary strategies for joint certification and accreditation of the Department's IT priority projects, and discuss these issues above. Though the preliminary strategies that IRM officials cited are a start, as discussed above, IRM and DS have not developed detailed and documented strategies on how the certification and accreditation process will be applied to help manage CCP information security risks.

IRM and DS provided conflicting responses to Recommendation 2, also directed to both bureaus. Specifically, IRM officials agreed with the recommendation, stating that CCP managers are currently soliciting contingency plans from locations that have modern C-LAN equipment as a means of developing a template to facilitate plan creation at other posts. IRM officials further stated that foreign affairs guidance already requires coordination of IT contingency plans with emergency action plans and that they are working closely with DS officials in this regard. In their response, however, DS officials stated that, per agreements with the Office of Management, oversight of the development and implement of security and contingency plans is the responsibility of IRM, not DS. We recognize the division in computer security roles and responsibilities and take no issue with this in our report. Rather, as discussed above, our concern focuses on the existence of redundant IT contingency programs and toolkits—including technical training provided by the DS Training Center—and the lack of adequate IT contingency plans at all overseas posts. We have revised our report to recommend that IRM coordinate and consolidate its IT contingency planning program with related activities in other Department organizations to help promote consistent IT contingency planning to support not just the CCP, but the Department's overall IT infrastructure.

APPENDIX A

PURPOSE, SCOPE, AND METHODOLOGY

The number one goal in the Department's Strategic IT Plan, FY 2001-FY 2005, is instituting a secure global communications network and IT infrastructure to help meet the challenge of e-diplomacy in the new millennium. The CCP is helping to meet this challenge by providing a commercial-style network and modern hardware and software for classified information processing and exchange at the desktop level. The Secretary's call for enhanced capabilities in the Department through the use of state of the art information technology provides the impetus for accomplishing the CCP within the next 2 years.

In accordance with our goal of helping to ensure more effective, efficient, and secure operations and infrastructures within the Department, OIG conducted a review of the Department's approach to CCP implementation. Specific objectives of our survey were to: (1) determine what, if any, security or operational problems are inherent in current classified local area networks overseas; (2) assess the Department's approach to planning and implementing its C-LAN systems modernization via the Classified Connectivity Program; and (3) identify what changes may be needed to the Department's modernization approach.

To fulfill our review objectives, we conducted web research to obtain background information on the Department's existing C-LAN infrastructure overseas, ongoing activities to improve classified connectivity, and criteria to govern these modernization activities. We examined a range of IT and security guidance, including Federal laws and policies, executive directives, Department regulations, and accepted project methodologies, that could be applied to the C-LAN implementation approach. We used these criteria to assess CCP management information obtained through discussions with and documentation provided by officials from various offices within IRM.

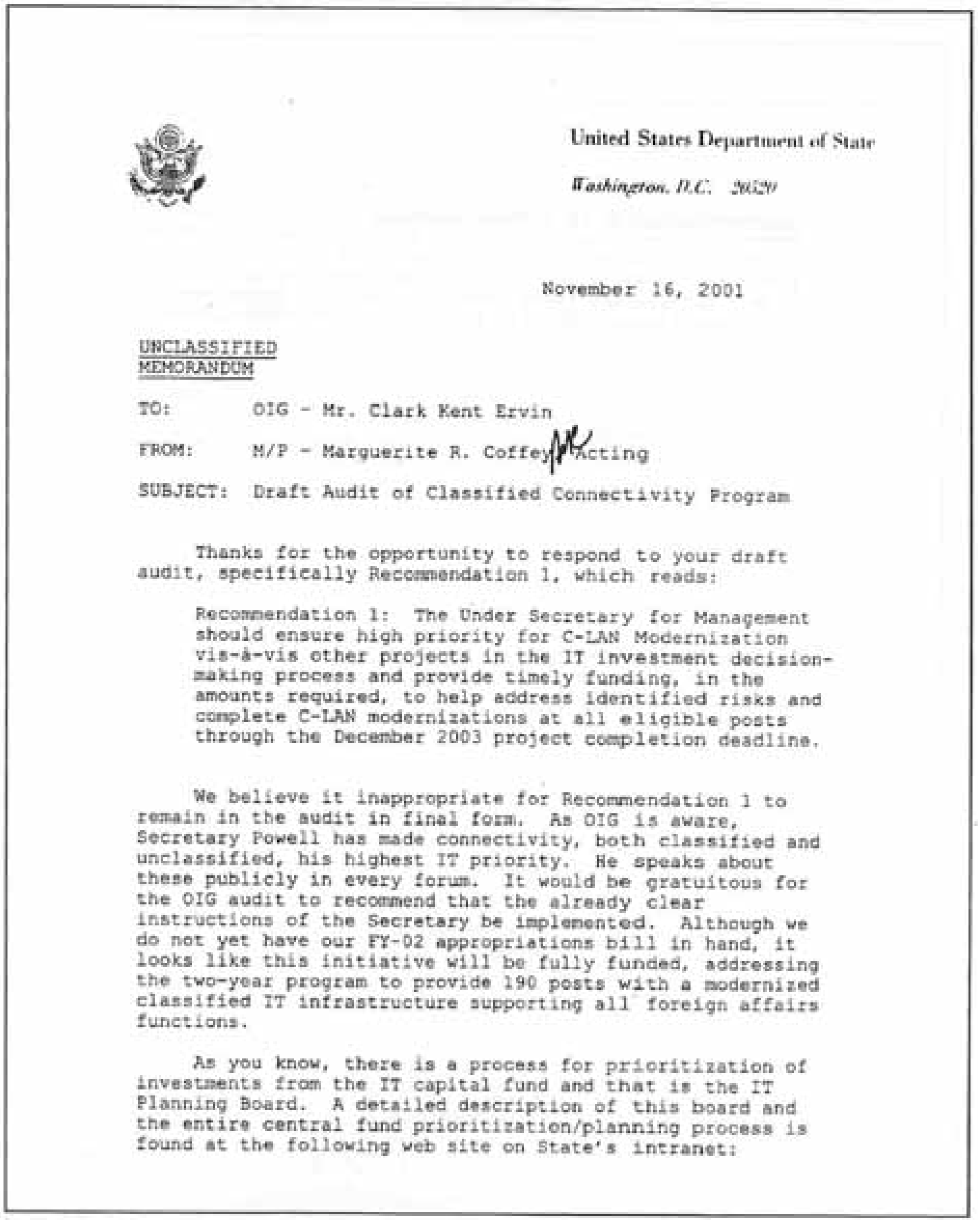
We also met with DS officials to discuss the Department's approach to identifying the risks and managing the security of the classified system. We interviewed officials in the Bureau of Administration to talk about CCP acquisition and logistics management issues. Senior managers in the Bureau of Financial Management and Policy told us about funding and budgeting for the program. Officials in DTS-PO told us about plans to provide the bandwidth needed to support classified information processing overseas. Further, we met with officials from selected regional bureaus within the Department to learn about problems experienced with existing classified networks, their role in CCP implementation, and benefits derived from the modernization efforts.

This review was an initial, high-level evaluation of ongoing CCP activities to gain an understanding of the planning and implementation approach and to identify general areas for potentially improving program direction. As such, we limited our review to an assessment of efforts to deploy equipment for the CCP. We did not visit posts to assess actual CCP installations, operations, or maintenance. We also did not conduct full assessments of the related SIPRNET router-based network or applications such as CableXpress that the C-LAN will support.

We conducted our review from March to September 2001 at the Department in Washington, DC. We performed our work in accordance with generally accepted government auditing standards. Major contributors to this report were Frank Deffer, Sondra McCauley, Cassandra Moore, Tim Fitzgerald, and Sharon Hunter. Comments or questions about the report can be directed to Frank Deffer, IT Evaluations and Operations, at defferf@state.gov or (703) 284-2715.

APPENDIX B

DEPARTMENT COMMENTS



United States Department of State

Washington, D.C. 20520

November 16, 2001

UNCLASSIFIED
MEMORANDUM

TO: OIG - Mr. Clark Kent Ervin

FROM: M/P - Marguerite R. Coffey, Acting

SUBJECT: Draft Audit of Classified Connectivity Program

Thanks for the opportunity to respond to your draft audit, specifically Recommendation 1, which reads:

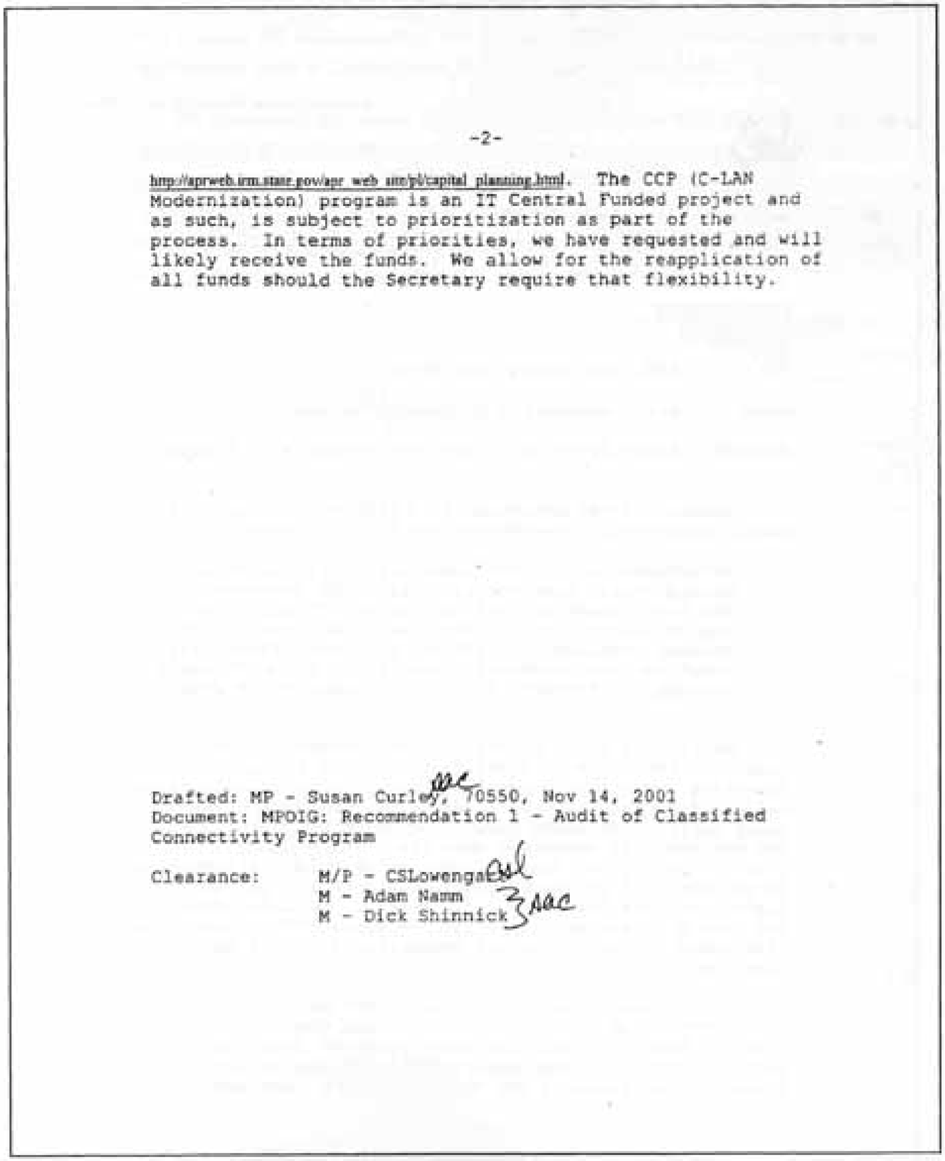
> Recommendation 1: The Under Secretary for Management should ensure high priority for C-LAN Modernization vis-à-vis other projects in the IT investment decision-making process and provide timely funding, in the amounts required, to help address identified risks and complete C-LAN modernizations at all eligible posts through the December 2003 project completion deadline.

We believe it inappropriate for Recommendation 1 to remain in the audit in final form. As OIG is aware, Secretary Powell has made connectivity, both classified and unclassified, his highest IT priority. He speaks about these publicly in every forum. It would be gratuitous for the OIG audit to recommend that the already clear instructions of the Secretary be implemented. Although we do not yet have our FY-02 appropriations bill in hand, it looks like this initiative will be fully funded, addressing the two-year program to provide 190 posts with a modernized classified IT infrastructure supporting all foreign affairs functions.

As you know, there is a process for prioritization of investments from the IT capital fund and that is the IT Planning Board. A detailed description of this board and the entire central fund prioritization/planning process is found at the following web site on State's intranet:

APPENDIX B

DEPARTMENT COMMENTS (Continued)



-2-

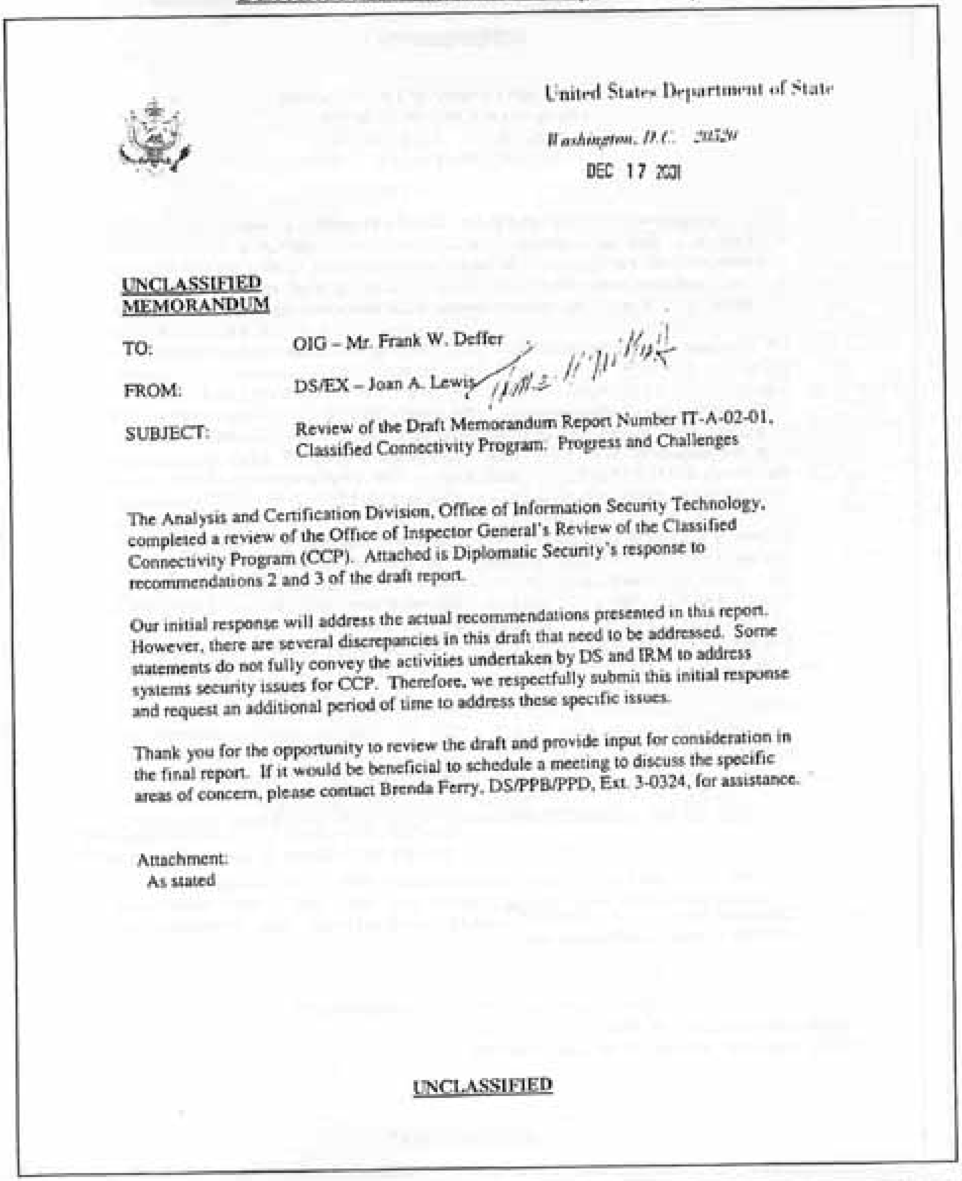
http://aprweb.irm.state.gov/apr web site/pl/capital planning.html. The CCP (C-LAN Modernization) program is an IT Central Funded project and as such, is subject to prioritization as part of the process. In terms of priorities, we have requested and will likely receive the funds. We allow for the reapplication of all funds should the Secretary require that flexibility.

Drafted: MP - Susan Curley, aac 70550, Nov 14, 2001
Document: MPOIG: Recommendation 1 - Audit of Classified Connectivity Program

Clearance: M/P - CSLowenga
M - Adam Namm
M - Dick Shinnick AAC

APPENDIX B

DEPARTMENT COMMENTS (Continued)



United States Department of State

Washington, D.C. 20520

DEC 17 2001

UNCLASSIFIED
MEMORANDUM

TO: OIG – Mr. Frank W. Deffer

FROM: DS/EX – Joan A. Lewis

SUBJECT: Review of the Draft Memorandum Report Number IT-A-02-01, Classified Connectivity Program: Progress and Challenges

The Analysis and Certification Division, Office of Information Security Technology, completed a review of the Office of Inspector General's Review of the Classified Connectivity Program (CCP). Attached is Diplomatic Security's response to recommendations 2 and 3 of the draft report.

Our initial response will address the actual recommendations presented in this report. However, there are several discrepancies in this draft that need to be addressed. Some statements do not fully convey the activities undertaken by DS and IRM to address systems security issues for CCP. Therefore, we respectfully submit this initial response and request an additional period of time to address these specific issues.

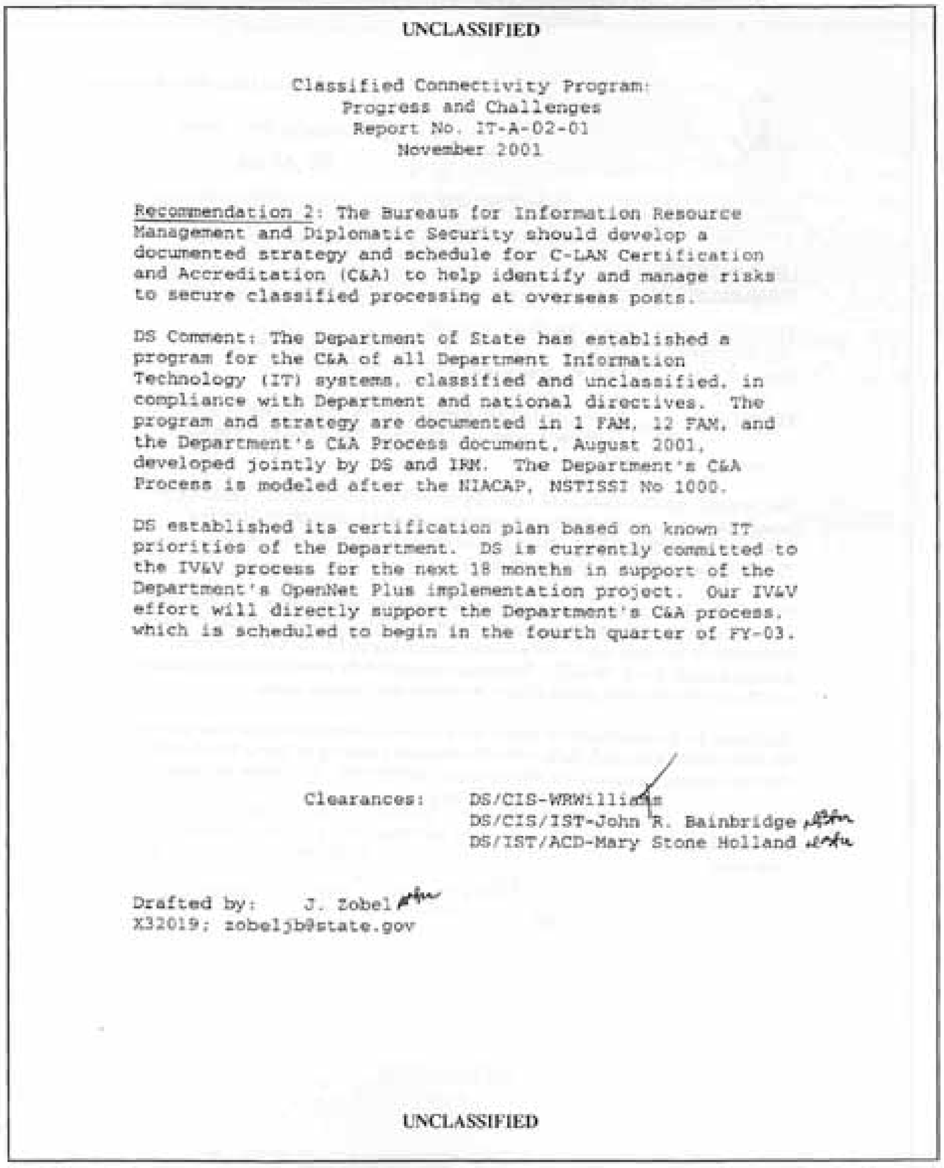
Thank you for the opportunity to review the draft and provide input for consideration in the final report. If it would be beneficial to schedule a meeting to discuss the specific areas of concern, please contact Brenda Ferry, DS/PPB/PPD, Ext. 3-0324, for assistance.

Attachment:
As stated

UNCLASSIFIED

APPENDIX B

DEPARTMENT COMMENTS (Continued)



UNCLASSIFIED

Classified Connectivity Program:
Progress and Challenges
Report No. IT-A-02-01
November 2001

Recommendation 2: The Bureaus for Information Resource Management and Diplomatic Security should develop a documented strategy and schedule for C-LAN Certification and Accreditation (C&A) to help identify and manage risks to secure classified processing at overseas posts.

DS Comment: The Department of State has established a program for the C&A of all Department Information Technology (IT) systems, classified and unclassified, in compliance with Department and national directives. The program and strategy are documented in 1 FAM, 12 FAM, and the Department's C&A Process document, August 2001, developed jointly by DS and IRM. The Department's C&A Process is modeled after the NIACAP, NSTISSI No 1000.

DS established its certification plan based on known IT priorities of the Department. DS is currently committed to the IV&V process for the next 18 months in support of the Department's OpenNet Plus implementation project. Our IV&V effort will directly support the Department's C&A process, which is scheduled to begin in the fourth quarter of FY-03.

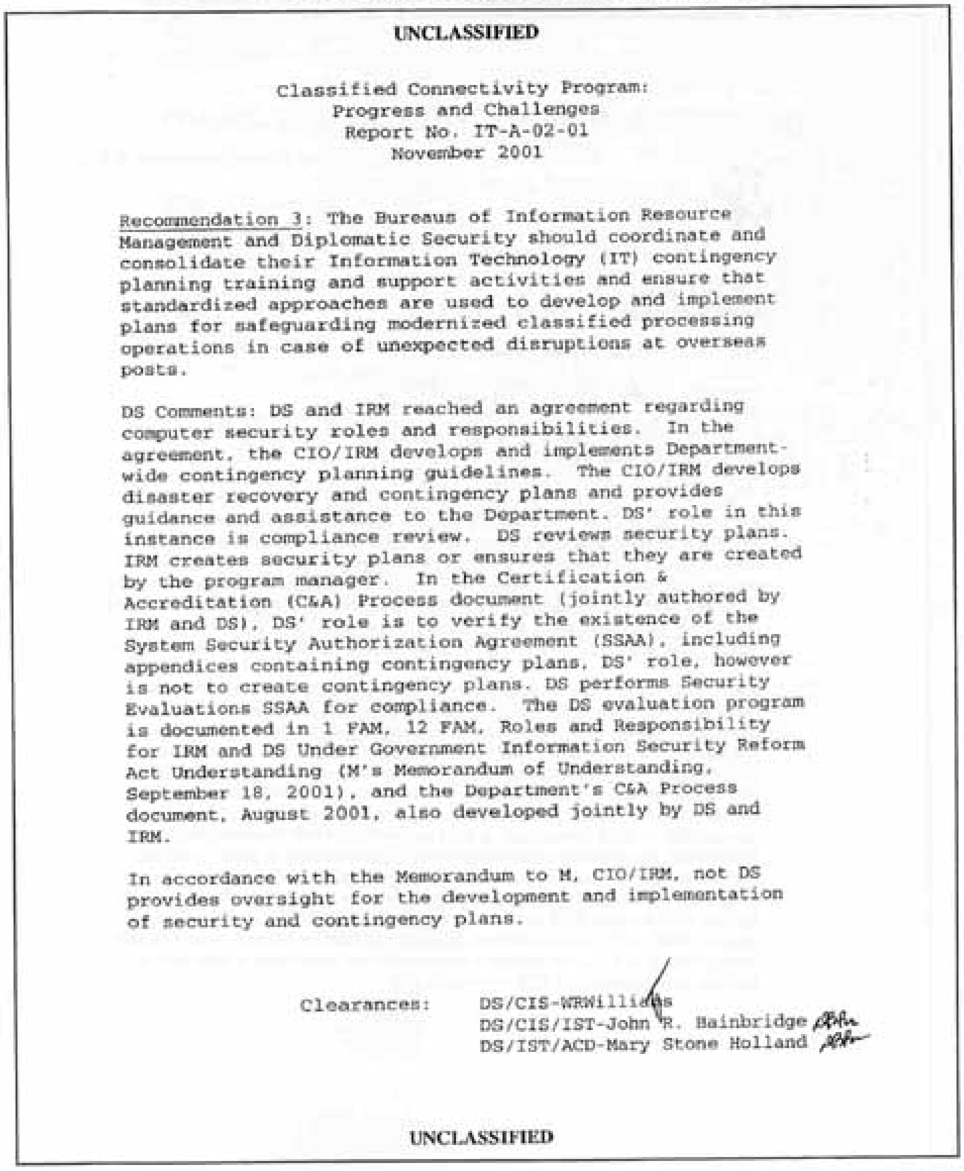
Clearances: DS/CIS-WRWilliams
DS/CIS/IST-John R. Bainbridge
DS/IST/ACD-Mary Stone Holland

Drafted by: J. Zobel
X32019; zobeljb@state.gov

UNCLASSIFIED

APPENDIX B

DEPARTMENT COMMENTS (Continued)



UNCLASSIFIED

Classified Connectivity Program:
Progress and Challenges
Report No. IT-A-02-01
November 2001

Recommendation 3: The Bureaus of Information Resource Management and Diplomatic Security should coordinate and consolidate their Information Technology (IT) contingency planning training and support activities and ensure that standardized approaches are used to develop and implement plans for safeguarding modernized classified processing operations in case of unexpected disruptions at overseas posts.

DS Comments: DS and IRM reached an agreement regarding computer security roles and responsibilities. In the agreement, the CIO/IRM develops and implements Department-wide contingency planning guidelines. The CIO/IRM develops disaster recovery and contingency plans and provides guidance and assistance to the Department. DS' role in this instance is compliance review. DS reviews security plans. IRM creates security plans or ensures that they are created by the program manager. In the Certification & Accreditation (C&A) Process document (jointly authored by IRM and DS), DS' role is to verify the existence of the System Security Authorization Agreement (SSAA), including appendices containing contingency plans. DS' role, however is not to create contingency plans. DS performs Security Evaluations SSAA for compliance. The DS evaluation program is documented in 1 FAM, 12 FAM, Roles and Responsibility for IRM and DS Under Government Information Security Reform Act Understanding (M's Memorandum of Understanding, September 18, 2001), and the Department's C&A Process document, August 2001, also developed jointly by DS and IRM.

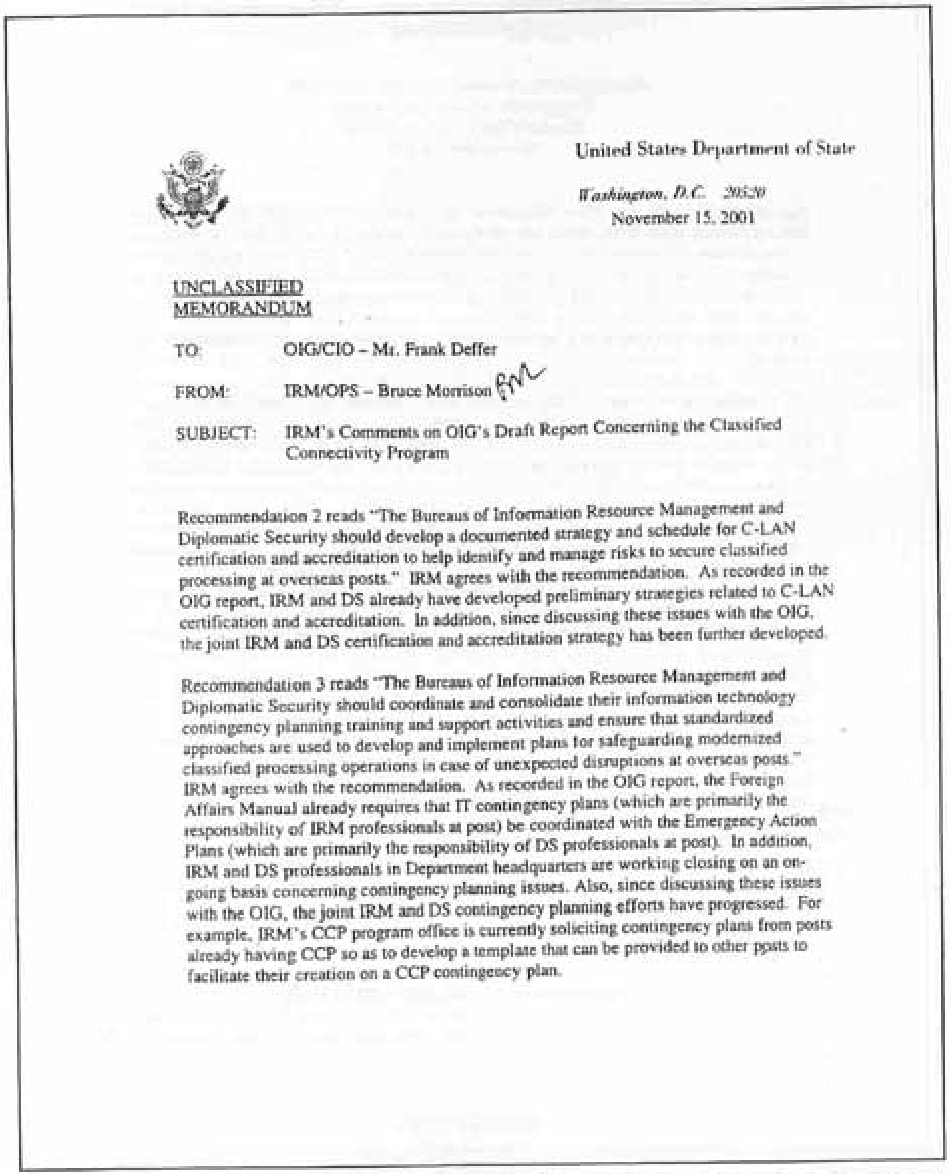
In accordance with the Memorandum to M, CIO/IRM, not DS provides oversight for the development and implementation of security and contingency plans.

Clearances: DS/CIS-WRWilliams
DS/CIS/IST-John R. Bainbridge
DS/IST/ACD-Mary Stone Holland

UNCLASSIFIED

APPENDIX B

DEPARTMENT COMMENTS (Continued)



United States Department of State

Washington, D.C. 20520
November 15, 2001

UNCLASSIFIED
MEMORANDUM

TO: OIG/CIO – Mr. Frank Deffer

FROM: IRM/OPS – Bruce Morrison

SUBJECT: IRM's Comments on OIG's Draft Report Concerning the Classified Connectivity Program

Recommendation 2 reads "The Bureaus of Information Resource Management and Diplomatic Security should develop a documented strategy and schedule for C-LAN certification and accreditation to help identify and manage risks to secure classified processing at overseas posts." IRM agrees with the recommendation. As recorded in the OIG report, IRM and DS already have developed preliminary strategies related to C-LAN certification and accreditation. In addition, since discussing these issues with the OIG, the joint IRM and DS certification and accreditation strategy has been further developed.

Recommendation 3 reads "The Bureaus of Information Resource Management and Diplomatic Security should coordinate and consolidate their information technology contingency planning training and support activities and ensure that standardized approaches are used to develop and implement plans for safeguarding modernized classified processing operations in case of unexpected disruptions at overseas posts." IRM agrees with the recommendation. As recorded in the OIG report, the Foreign Affairs Manual already requires that IT contingency plans (which are primarily the responsibility of IRM professionals at post) be coordinated with the Emergency Action Plans (which are primarily the responsibility of DS professionals at post). In addition, IRM and DS professionals in Department headquarters are working closing on an on-going basis concerning contingency planning issues. Also, since discussing these issues with the OIG, the joint IRM and DS contingency planning efforts have progressed. For example, IRM's CCP program office is currently soliciting contingency plans from posts already having CCP so as to develop a template that can be provided to other ppsts to facilitate their creation on a CCP contingency plan.