MEMORANDUM REPORT NUMBER IT-A-02-03

Challenges to Successful OpenNet Plus Implementation

March 2002

The OpenNet Plus program is intended to provide every employee of the Department of State (the Department) with desktop access to the Internet's World Wide Web. The Internet has become an indispensable source of information and a universal method for rapid communications among organizations engaged in government and business transactions worldwide. Department employees have also become increasingly dependent on the Internet to help them carry out their foreign affairs activities in a reliable, fast, and cost-effective manner.

In accordance with our goal of helping to ensure more effectiveness, efficiency, and security in the Department's information technology (IT) operations and infrastructure, OIG conducted a review of the OpenNet Plus program. This report focuses on the Department's approach to implementing OpenNet Plus domestically and at overseas embassies and consulates. Specific objectives of our review were to (1) determine whether the Department is adequately planning and managing deployment of OpenNet Plus, (2) determine whether the Department has taken adequate steps to ensure security of the OpenNet Plus infrastructure, and (3) identify plans and procedures for monitoring and ensuring proper use of the Internet in accordance with established policy guidelines. The purpose, scope, and methodology for our review are discussed in Appendix A.

RESULTS IN BRIEF

Desktop access to the Internet will be invaluable in supporting Department employees with the information and communications needed to carry out their foreign affairs responsibilities on a day-to-day basis. The Department is taking a structured approach to implementing OpenNet Plus, its program for providing this long-awaited capability. The approach includes a deliberate process for ensuring that bureaus and overseas missions meet established technical, physical, security, and management requirements for Internet access before they are granted connectivity through OpenNet Plus.

However, the Department has not instituted all of the policies needed to support OpenNet Plus implementation—particularly with regard to eliminating redundant Internet connections once OpenNet Plus is deployed and monitoring employee use of the Internet. By instituting the necessary policies, the Department will be able to avoid duplicative costs arising from maintaining separate Internet networks. Establishment of a specific Internet monitoring policy and approach will also minimize the potential for inappropriate use of the Internet in the workplace, and corresponding wasted time and taxpayer dollars.

BACKGROUND

The OpenNet Plus project is intended to address the Secretary's commitment to providing, as soon as possible, all Department employees with desktop access to the Internet's World Wide Web to help carry out the foreign affairs mission. Access to the Internet is being accomplished via the Department's existing global Open Network (OpenNet) infrastructure. OpenNet serves as the foundation for sensitive but unclassified information processing and communications among headquarters organizations and over 260 locations worldwide and is used by most employees for typical day-to-day operations and for e-mail. This network is mirrored on the classified side of the Department by a second network that supports secure office automation, e-mail, and limited web-based communications up to the secret level.

The OpenNet Plus program was preceded by a history of repeated efforts to provide Internet access at the desktop. During the early 1990s, given the proliferation of personal computers and the increasing number of people turning to the Internet for communications and research, the requirement for greater Internet access in the Department became apparent. Questions were raised concerning how to provide Internet access at the desktop for Department users in a secure manner. Consequently, during the summer of 1996, the Bureau of Diplomatic Security (DS) performed a risk assessment to determine whether the OpenNet infrastructure was secure enough to support Internet service. DS completed its assessment, identifying a number of vulnerabilities related to OpenNet access control, configuration management, and security oversight. At that point, the Department decided not to move forward with plans for providing Internet access at the desktop, but to retain Internet e-mail service only within the existing OpenNet infrastructure.

Given the vulnerabilities that DS identified with OpenNet, in 1996-97 the Bureau of Information Resource Management (IRM) conducted a pilot test to determine the feasibility of implementing another infrastructure for providing much-needed Internet service. As a result of the pilot, IRM instituted a third network, the Rich Internet Access Network, which provided Internet access on a fee-for-service basis for domestic organizations that requested it. Rich Internet Access costs approximately $5,400 per person to cover requirements for additional desktop computers, as well as network support and administrative overhead. At the same time that Rich Internet Access was deployed, bureaus, offices, embassies, and consulates were implementing their own independent Internet access solutions. These included dedicated Internet local area networks and stand-alone Internet terminals.

With the integration of the United States Information Agency into the Department on October 1, 1999, a fourth network was introduced, which also provided Internet access. This network, Public Diplomacy Network, is used for unclassified information processing and communications by employees within the Office of the Under Secretary for Public Diplomacy and Public Affairs. With this addition, senior managers became concerned about the enormous cost of maintaining an IT infrastructure that includes four separate networks. In 1999, the Department established a team to research and consider alternative strategies for eliminating some of the redundancies and providing cost-effective Internet solutions. The following year, the Under Secretary for Management approved a 90-day pilot program for the OpenNet Plus project, which permitted IRM employees to access the Internet at their desktops.

Although initially limited in its Internet access capabilities, OpenNet Plus is intended to provide a range of services previously unavailable to all Department employees. For example, the program will provide desktop access to thousands of public and private web sites, such as firstgov.gov and washingtonpost.com. OpenNet Plus will also support electronic transactions, such as purchasing computer equipment from online suppliers or buying books via amazon.com. Further, OpenNet Plus will enable collaboration among foreign affairs agencies as part of the Department's Foreign Affairs Systems Integration initiative, as well as provide a strong foundation for modern "e-government" operations in accordance with requirements of the Government Paperwork Elimination Act. Additional Internet services will be added to OpenNet Plus as the program evolves and as new requirements, technologies, and effective security techniques are developed.

REVIEW FINDINGS

STRUCTURED APPROACH TO OPENNET PLUS IMPLEMENTATION

The Department is taking a structured approach to implementing OpenNet Plus. This approach began with a pilot program, conducted from January through April 2001 with the participation of approximately 400 IRM employees. During the pilot program, a contractor performed a vulnerability assessment of the Department's systems security while IRM users were connected to the Internet. The study revealed some security and administrative weaknesses currently being addressed by DS and IRM.

Upon successful completion of the pilot, IRM established the OpenNet Plus Project Management Office (PMO) to develop, execute, manage, and monitor the program from the initial planning phase begun in May 2001 through the installation phase, expected to be completed in May 2003. A major PMO responsibility is coordinating with Department bureaus and overseas missions on a regular basis to help them prepare for connection to the Internet. The Department authorized $6.2 million for OpenNet Plus rollout in May 2001 and, through its Information Technology investment decisionmaking process for FY 2002, expects to allocate $109 million to support deployment. The PMO provides monthly updates to the Under Secretary for Management and the Chief Information Officer (CIO), the program sponsor, on OpenNet Plus funding issues and progress toward meeting established milestones and objectives.

According to foreign affairs regulations,[1] the Managing State Projects methodology must be used for managing the development of all IT projects that exceed one year and cost over $500,000. In compliance with these regulations, the PMO used the methodology to help develop a draft of the OpenNet Plus Project Plan in October 2001. The plan outlines the resources and timelines needed for OpenNet Plus deployment domestically and overseas. Based on the Managing State Projects concept, the program will include five major phases—study, acquisition, integration, deployment, and installation.

[1] Foreign Affairs Manual, chapter 5, section 621

The PMO's initial strategy for OpenNet Plus deployment included development of a Connection Approval Process workbook, which outlines the procedures that a bureau, embassy, or consulate must follow to obtain approval for Internet access through the program. The entire connection approval process consists of multiple steps to ensure that each Department organization meets information security requirements. These steps also aid in the development of a technical strategy for making the connection to OpenNet Plus. The initial steps that must be completed include:

- Designating and training Information Systems Security Officers to manage the organization's IT security program;
- Complying with systems security configuration guidelines;
- Initiating development of IT contingency plans;
- Controlling and standardizing systems configuration and change management procedures;
- Verifying compliance with hardware and software baseline configurations to support a common operating environment; and
- Ensuring that end users complete the required security training.

After a bureau or overseas mission has completed these initial steps in the Connection Approval Process workbook, DS performs an independent verification and validation of the site's systems and physical and technical environments. The independent verification and validation, conducted in accordance with foreign affairs guidance,[2] provides assurance that basic security controls are in place prior to connection to OpenNet Plus. DS can perform independent verification and validation either remotely, using technical tools and methodologies, or on-site at the individual Department organization. Because of time constraints, DS may in some instances use remote tools to initiate the independent verification and validation process. DS will coordinate with regional security officers on the physical and administrative aspects of the process for those posts that undergo remote independent verification and validation. DS will be unable to perform independent verification and validation on-site at all embassies and consulates, but hopes to visit at least 60 percent of all overseas locations to do the tests.

[2] Foreign Affairs Manual, chapter 12, section 600

As a result of independent verification and validation, DS can determine whether a bureau, embassy, or consulate is in compliance with all connection approval process requirements. If fully compliant, DS recommends that the CIO—the Designated Approving Authority—grant "interim authority to operate," or temporary approval for connection to OpenNet Plus. If not compliant with the connection approval process requirements, the bureau or overseas mission must first meet all requirements before the interim authority to operate is granted. In addition to meeting all connection approval process requirements, Internet connection is contingent upon an organization's having adequate bandwidth—the telecommunications capacity required to support data transfer. The Diplomatic Telecommunications Service Program Office is the Department's preferred bandwidth supplier for overseas sites. If the Diplomatic Telecommunications Service Program Office cannot supply the technically required bandwidth within the established time frame, the OpenNet Plus Program Office will obtain bandwidth via satellite or local Internet service providers. In June 2001, IRM developed a capacity plan outlining the Department's bandwidth requirements worldwide.

The final step in the connection approval process is a series of internal processes that IRM must complete before activating OpenNet Plus at a given location. These processes include reviewing independent verification and validation reports, validating bandwidth availability, and issuing compliance agreements for management signature. As of the end of November 2001, the Bureau of Economic and Business Affairs, part of IRM, the Warrenton Training Center,[3] and Embassy Nicosia had been connected to OpenNet Plus. In addition, parts of Embassy New Delhi, Embassy Mexico City, and domestic organizations included in the Department's Foreign Affairs Systems Integration pilot program have also received access to OpenNet Plus, which is needed to support web-based data sharing and exchange among foreign affairs agencies.

After connection to OpenNet Plus, a bureau or overseas mission must prepare for certification and accreditation—a structured process for ensuring IT security risk management in compliance with Department and federal directives. Specifically, "certification" is the independent, comprehensive evaluation of the technical and non-technical security features of an information system. "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 minimum standards, activities, and

[3] This training center, located in Warrenton, Virginia, is part of the Foreign Service Institute's School of Applied Information Technology.

management structure for certification and accreditation are prescribed in the National Information Assurance Certification and Accreditation Process developed by the National Security Telecommunications and Information Systems Security Committee. This document also outlines the roles and responsibilities of those involved in the process. Within the Department, DS serves as the Certification Authority responsible for determining the level of residual security risk to an IT system and making an accreditation recommendation to the CIO, who is the Designated Approving Authority. All bureaus and overseas missions must complete the certification and accreditation process to maintain their connection to OpenNet Plus.

In accordance with requirements of the National Information Assurance Certification and Accreditation Process, each Department organization undergoing OpenNet Plus certification and accreditation must also develop a systems security authorization agreement. The agreement, initiated at the beginning of an IT project, is used to guide certification and accreditation activities and document agreement among the certifier, approving authority, user representative, and program manager to support the risk management process. The agreement is a compilation of various documents, including a description of the IT operating environment, a systems security architecture, test plans and procedures, and certification results, that form the baseline security configuration document. In the case of OpenNet Plus, each organization must complete specific portions of the systems security authorization agreement no later than nine months from the date that the interim authority to operate is granted.

ADDITIONAL POLICIES NEEDED TO SUPPORT OPENNET PLUS IMPLEMENTATION

The Department has not yet instituted all of the policy guidance needed to govern OpenNet Plus implementation. The OpenNet Plus PMO has taken a step in this direction by identifying nine areas in which policies are needed to define and manage effectively the OpenNet Plus global infrastructure. These areas include asset management, systems architecture and configuration standards, network monitoring, and security.

Currently, some guidance exists in a few of the areas identified. Specifically, the Department's foreign affairs manuals include fairly comprehensive guidance regarding software development, project management, and configuration management. However, the guidance is limited with regard to roles and responsibilities and internal controls for managing agency-wide IT programs such as OpenNet Plus. The PMO has begun to map the existing guidance to a “Leading Policy Practice Framework,” which provides a strategy for enhancing the guidance or developing new policies to support the OpenNet Plus program. For areas where no guidance currently exists, the framework identifies target policies and establishes priorities for their immediate or long-term development. According to the draft OpenNet Plus project plan, the PMO will develop the required policies over the next 18 months.

OIG believes that continued progress in policy development is critical, especially in two key areas. The first area involves having Department organizations eliminate existing Internet connections after OpenNet Plus has been deployed. Currently, the acquisition of Internet access is decentralized, allowing organizations to select from a variety of methods to obtain such services. Domestically, bureaus have web access through IRM’s Rich Internet Access, Internet Local Area Networks, stand-alone dial-up connections, and the Public Diplomacy Network. With the exception of IRM’s Rich Internet Access, overseas embassies and consulates also use these same means to access the Internet. In many cases, Internet access requires that an employee have an additional workstation on the desktop or use shared terminals. OpenNet Plus deployment, as previously discussed, is intended to standardize how the Department acquires Internet service and eliminate the need for separate networks and workstations.

In the absence of a central policy several bureaus and overseas missions have indicated that they expect to keep their separate Internet connections after OpenNet Plus is implemented, resulting in redundant capabilities. Their reasons for keeping the existing connections include having back-up Internet service in case OpenNet Plus becomes unavailable or ensuring additional capabilities (i.e., remote log-in and audio- and video-streaming) that currently are not offered through the OpenNet Plus program.

Based on our preliminary analysis of selected Department data on Internet service costs, overseas missions are spending almost one million dollars per year to maintain their separate Internet connections. To eliminate the duplicative Internet service costs, the Department needs to institute a policy requiring that bureaus, offices, embassies, and consulates discontinue or shut down their independent Internet connections after OpenNet Plus is implemented, unless a business case is provided to justify continued use. The Director of the OpenNet Plus PMO recently stated that a policy is being drafted and will be presented to the Department’s IT Change Control Board for review. This board, created in October 2001 and chaired by IRM, manages changes to the Department’s global environment.

Recommendation 1: We recommend that the Bureau of Information Resource Management develop and implement a policy that directs bureaus, offices, embassies, and consulates to terminate existing Internet services once OpenNet Plus is deployed. The policy should include how long legacy Internet connections may remain in service during the transition to OpenNet Plus. The policy should also outline how a bureau, office, embassy, or consulate can petition to keep its existing Internet connections by making a detailed business case.

A second area of OIG concern is the sensitive issue of monitoring employee use of the Internet within the Department. As with any other organization providing Internet service at the desktop, such access can result in employee misuse and/or abuse. Employees can spend large periods of government time using the Internet for personal reasons and/or accessing inappropriate sites. Various publications identified a number of instances where employees in some industries and government agencies accessed the Internet at work for pleasure or to conduct personal business. This can lead to workplace inefficiencies, wasted taxpayers' dollars, hostile work environments, and lawsuits. Even with the limited Internet access currently available, the Department has already experienced some abuse by its employees. For example, a Foreign Service officer assigned overseas was suspended for ten days for using a government computer to access a pornographic web site.

The Department has taken some steps that begin to address this issue. Specifically, in March 2000, the Under Secretary for Management instituted a policy that allows employees limited use of government equipment for personal reasons.[4] Included in this policy is use of the Internet, as long as it does not result in increased cost to the Department. Employees are allowed to use the Internet in moderation on personal time for matters that are not directly related to official business. The policy also states, however, that employees can have no expectation of privacy while using any government-provided Internet service. Employees are also to conduct themselves professionally in the workplace and to refrain from using Department resources for activities that may be offensive to coworkers or the public. These policies are outlined in several foreign affairs regulations, some of which are awaiting final clearance.[5]

[4] Department Notice 2000-03-35, "Personal Use of Government Equipment," March 17, 2000.

[5] Foreign Affairs Manual chapter 5, section 700 (awaiting clearance) and chapter 12, section 600, chapter 5 section 516.3-3.

Further, the Department is working to prevent employee access to inappropriate Internet web sites. Specifically, the Department has installed an off-the-shelf software program that blocks access to certain sites. The software serves as a firewall, blocking user access to prohibited sites that contain nudity, sexually explicit material, profanity, gambling, or racist and sexist propaganda. In addition, the software gives the Department's Network Control Center the capability to block sites not contained in the software database. The database is updated daily to reflect any new sites or changes to existing ones. Because of incompatibility with another firewall, the content blocking software was off-line from October to late November 2001. During this period, the Department utilized manual means to regulate access to the Internet. IRM ultimately modified the firewall configuration to restore the software to service.

Instituting employee equipment use policies and the content blocking software are steps in the right direction. However, more is needed. Specifically the Department has no guidelines in place to address how or whether it will monitor employee compliance with existing use policies as they relate to the Internet. Before instituting such Internet monitoring, the Department will first have to determine the extent to which it is necessary and who will be responsible for conducting it. Further, the Department will also need a strategy to enforce compliance or address violations. Implementing the policies as OpenNet Plus is deployed should help eliminate problems before they arise. Such policies would also provide a general understanding of how IRM or supervisors will monitor Internet use and what repercussions employees will face if they abuse their Internet privileges.

Recommendation 2: We recommend that the Bureau of Information Resource Management, in collaboration with the Bureaus of Diplomatic Security and Human Resources, develop and implement specific policies that address how the Department will monitor Internet use by employees and the extent to which such monitoring will be done.

INFORMATION SECURITY ISSUES

Although OpenNet Plus will provide employees with ready access to a range of web information and resources, it will also pose potential IT security risks for the Department's data processing operations. As discussed above, desktop access to the Internet will be provided via the Department's OpenNet infrastructure, a sensitive but unclassified network that connects embassies, consulates, and domestic facilities to support global communications and services. This network contains proprietary and critical mission and business data—financial, personnel, foreign affairs, and visa information—that must be protected against loss, destruction, or compromise. Due to the sensitive nature of these issues, the details on our information security findings and recommendations will be included in a separate product.

DEPARTMENT COMMENTS AND OUR EVALUATION

We obtained written comments on a draft of this report from the Bureaus of Information Resource Management, Human Resources, and Diplomatic Security. We have included copies of the comments in their entirety at Appendix B.

In its response, IRM concurred with Recommendation 1 regarding terminating existing Internet connections once OpenNet Plus is deployed. IRM stated that the bureau has already drafted a policy in this regard, very similar to the suggestion outlined in our report. The next step will be to have the policy approved by the IT Change Control Board, chaired by IRM and comprised of executive representatives of organizations across the Department with responsibility for managing changes to the Department's global IT environment.

IRM agreed that Recommendation 2 concerning monitoring Internet usage addresses significant issues for the Department. However, IRM did not believe that it is in a lead position to develop and implement policies on such issues. IRM stated that it has taken responsibility on the prevention side by using technology to prevent employee access to Internet sites for illegitimate purposes. IRM also stated that the Department has existing policies to govern abuse of equipment such as telephones and that potential Internet abuse does not require a separate policy. Similarly, Human Resources also believed that Recommendation 2, directed to that bureau, is inappropriate. The bureau stated that the Department's Discipline Program, included in existing foreign affairs guidance, already outlines roles and responsibilities, enforcement procedures, and penalties for employees who abuse and/or misuse the Internet.

OIG agrees in part with the comments provided by IRM and Human Resources with regard to Recommendation 2 and has revised the recommendation, eliminating the requirement for additional personnel policies on Internet use. However, OIG believes that the Department still needs to assign responsibilities and develop guidelines for monitoring employee compliance with existing policies as they relate to Internet use. OIG also believes that the Discipline Program that Human Resources cited does not address how the Internet monitoring will be done. In addition, if the Department determines that line managers need to monitor employee use of the Internet, we agree with IRM's suggestion that training be provided in this regard.

In its comments, DS did not respond to Recommendation 2, which we directed to the bureau for action. DS only provided clarification on information security processes and requirements, which we have incorporated in the text above.

PURPOSE, SCOPE AND METHODOLOGY

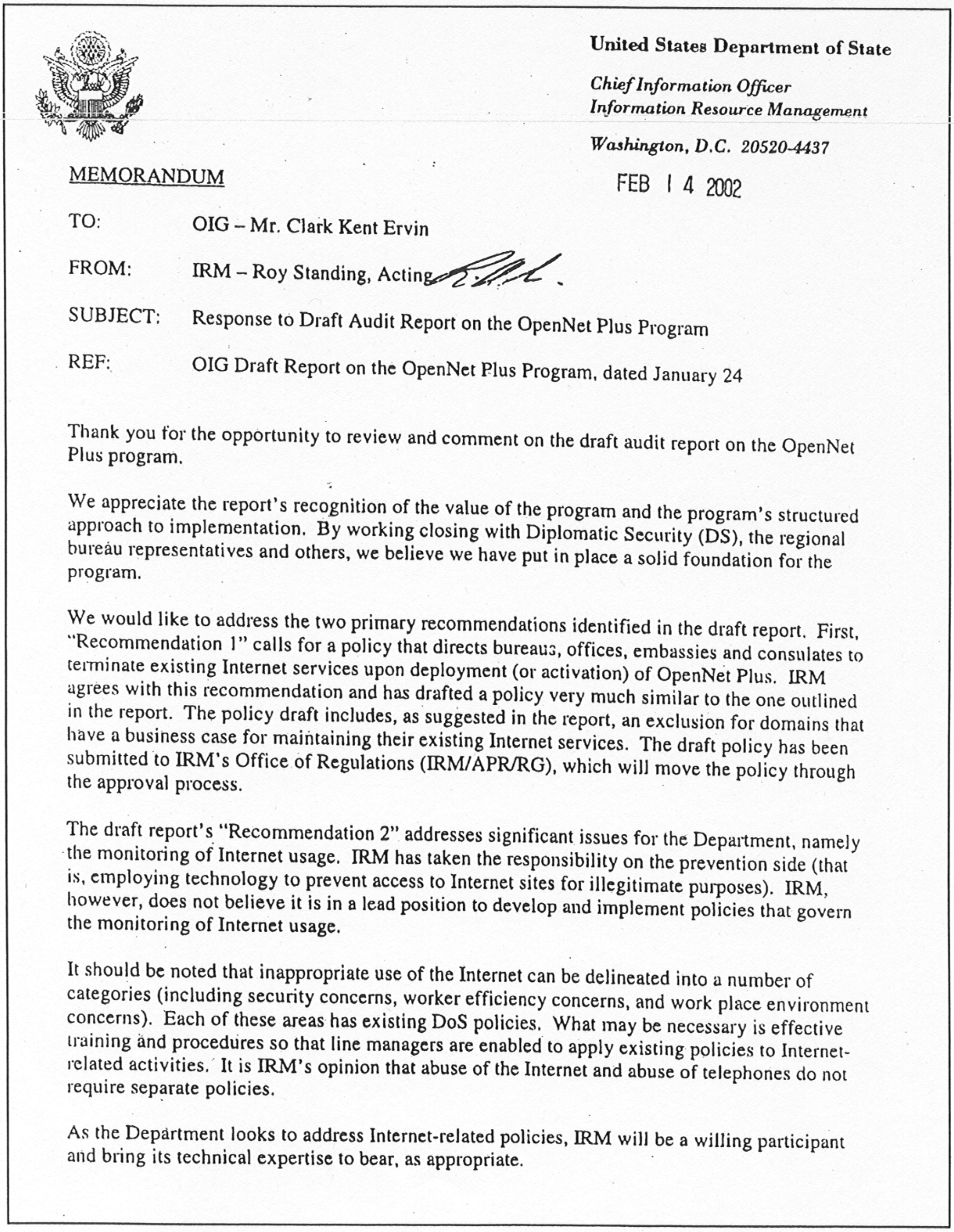
To fulfill our review objectives, we obtained background information on the existing OpenNet infrastructure, resources, and capabilities. We also studied networks currently in place to support Internet access—Public Diplomacy Network and Rich Internet Access Network—their capabilities, operations, and effective practices. We examined a range of IT and security guidance, including federal laws and policies and Departmental regulations applicable to the implementation and deployment of IT systems for web access.

We met with officials from IRM to discuss the Department's approach to identifying the risks, timelines, and resources needed for OpenNet Plus implementation. We attended OpenNet Plus weekly briefings to monitor the status of the program. We interviewed officials from the Office of International Information Programs to talk about their current network available to provide web access to Public Diplomacy users worldwide. We also met with officials from DS to discuss the Department's plans for assessing IT security and possible solutions for managing the risks to installing OpenNet Plus at the desktop.

In conducting this review, we focused on assessing the results of the 90-day OpenNet Plus Pilot, which started in January 2001, and evaluating the Department's plans for initial deployment of OpenNet Plus. We did not visit embassies or consulates to assess local capabilities, security risks, or current web access network configurations.

We conducted our review from May to November 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, John Shiffer, and Maria Cunningham. Comments or questions about the report can be directed to Mr. Deffer, IT Evaluations and Operations, at defferf@state.gov or (703) 284-2715.

DEPARTMENT COMMENTS



United States Department of State

Chief Information Officer
Information Resource Management

Washington, D.C. 20520-4437

MEMORANDUM

FEB 1 4 2002

TO: OIG – Mr. Clark Kent Ervin

FROM: IRM – Roy Standing, Acting

SUBJECT: Response to Draft Audit Report on the OpenNet Plus Program

REF: OIG Draft Report on the OpenNet Plus Program, dated January 24

Thank you for the opportunity to review and comment on the draft audit report on the OpenNet Plus program.

We appreciate the report's recognition of the value of the program and the program's structured approach to implementation. By working closing with Diplomatic Security (DS), the regional bureau representatives and others, we believe we have put in place a solid foundation for the program.

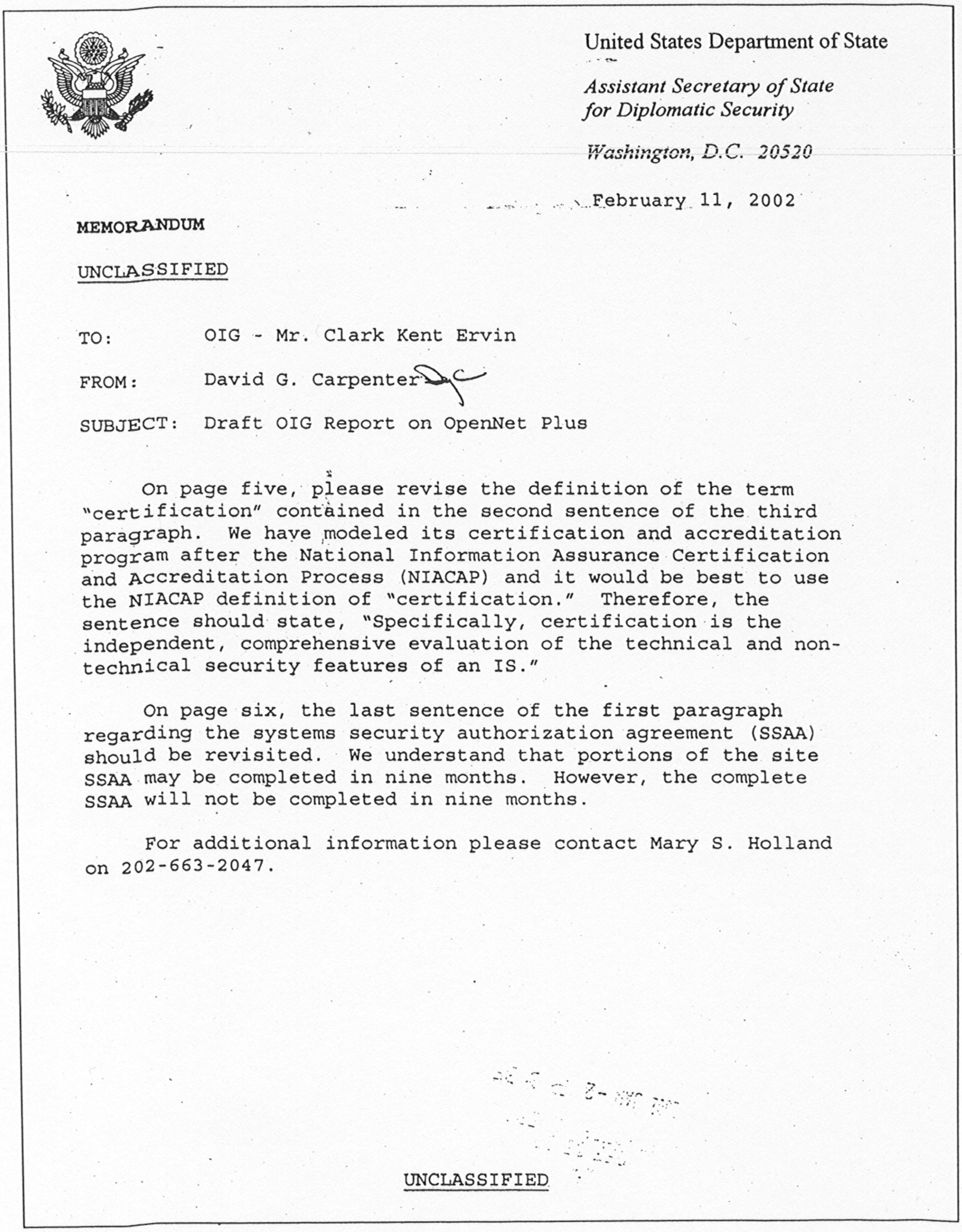
We would like to address the two primary recommendations identified in the draft report. First, "Recommendation 1" calls for a policy that directs bureaus, offices, embassies and consulates to terminate existing Internet services upon deployment (or activation) of OpenNet Plus. IRM agrees with this recommendation and has drafted a policy very much similar to the one outlined in the report. The policy draft includes, as suggested in the report, an exclusion for domains that have a business case for maintaining their existing Internet services. The draft policy has been submitted to IRM's Office of Regulations (IRM/APR/RG), which will move the policy through the approval process.

The draft report's "Recommendation 2" addresses significant issues for the Department, namely the monitoring of Internet usage. IRM has taken the responsibility on the prevention side (that is, employing technology to prevent access to Internet sites for illegitimate purposes). IRM, however, does not believe it is in a lead position to develop and implement policies that govern the monitoring of Internet usage.

It should be noted that inappropriate use of the Internet can be delineated into a number of categories (including security concerns, worker efficiency concerns, and work place environment concerns). Each of these areas has existing DoS policies. What may be necessary is effective training and procedures so that line managers are enabled to apply existing policies to Internet-related activities. It is IRM's opinion that abuse of the Internet and abuse of telephones do not require separate policies.

As the Department looks to address Internet-related policies, IRM will be a willing participant and bring its technical expertise to bear, as appropriate.

DEPARTMENT COMMENTS (continued)



United States Department of State

Assistant Secretary of State
for Diplomatic Security

Washington, D.C. 20520

February 11, 2002

MEMORANDUM

UNCLASSIFIED

TO: OIG - Mr. Clark Kent Ervin

FROM: David G. Carpenter

SUBJECT: Draft OIG Report on OpenNet Plus

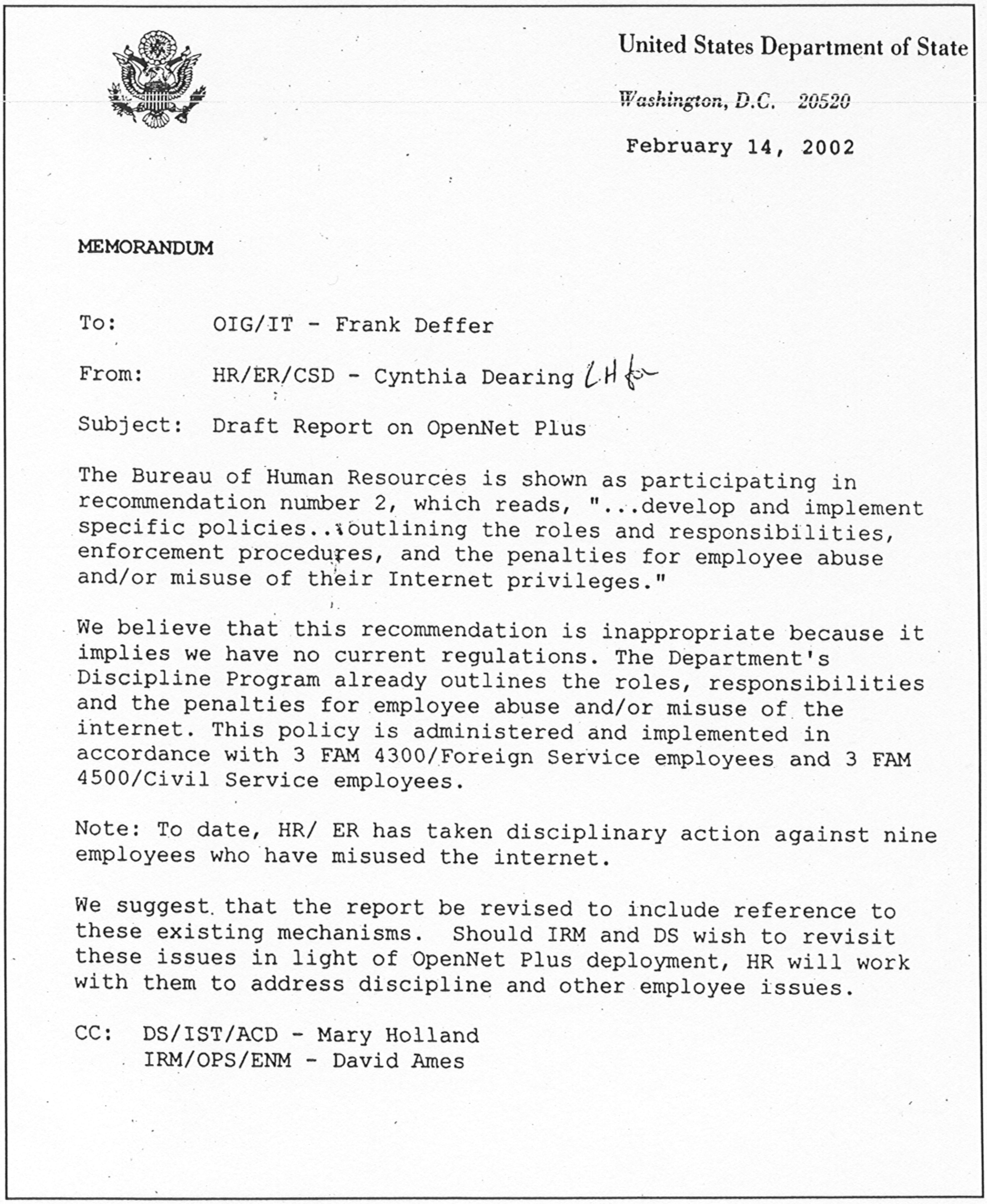
On page five, please revise the definition of the term "certification" contained in the second sentence of the third paragraph. We have modeled its certification and accreditation program after the National Information Assurance Certification and Accreditation Process (NIACAP) and it would be best to use the NIACAP definition of "certification." Therefore, the sentence should state, "Specifically, certification is the independent, comprehensive evaluation of the technical and non-technical security features of an IS."

On page six, the last sentence of the first paragraph regarding the systems security authorization agreement (SSAA) should be revisited. We understand that portions of the site SSAA may be completed in nine months. However, the complete SSAA will not be completed in nine months.

For additional information please contact Mary S. Holland on 202-663-2047.

UNCLASSIFIED

DEPARTMENT COMMENTS (continued)



United States Department of State

Washington, D.C. 20520

February 14, 2002

MEMORANDUM

To: OIG/IT - Frank Deffer

From: HR/ER/CSD - Cynthia Dearing LH for

Subject: Draft Report on OpenNet Plus

The Bureau of Human Resources is shown as participating in recommendation number 2, which reads, "...develop and implement specific policies...outlining the roles and responsibilities, enforcement procedures, and the penalties for employee abuse and/or misuse of their Internet privileges."

We believe that this recommendation is inappropriate because it implies we have no current regulations. The Department's Discipline Program already outlines the roles, responsibilities and the penalties for employee abuse and/or misuse of the internet. This policy is administered and implemented in accordance with 3 FAM 4300/Foreign Service employees and 3 FAM 4500/Civil Service employees.

Note: To date, HR/ ER has taken disciplinary action against nine employees who have misused the internet.

We suggest that the report be revised to include reference to these existing mechanisms. Should IRM and DS wish to revisit these issues in light of OpenNet Plus deployment, HR will work with them to address discipline and other employee issues.

CC: DS/IST/ACD - Mary Holland
IRM/OPS/ENM - David Ames