Office of Inspector General
U.S. Department of State
and the
Broadcasting Board of Governors

MONTHLY REPORT OF ACTIVITIES

audits, inspections, testimony, and special activities

June 2001

This report describes testimony provided by the Inspector General or other OIG officials and lists OIG reports issued during the period indicated. This report includes unclassified summaries of classified reports; all text in this report is unclassified. Classified reports are not distributed publicly. On occasion, OIG distributes an unclassified version of a classified report; in such a case, this listing also indicates the issued date of the original report. In addition, all major reports, together with OIG investigative activities, are summarized in the Inspector General's semiannual reports to the Congress, which are publicly available every June and December.

Congressional and Outreach Activities

Testimony

On June 27, 2001, the Senate Foreign Relations Committee held a confirmation hearing for four State Department presidential nominees. Among them was Clark Kent Ervin, the President's nominee to be Inspector General of the State Department. Mr. Ervin was introduced by Senators Kay Bailey Hutchison and Phil Gramm of Texas, both of whom gave strong endorsements.

Reports Issued Relating to Financial Management and Administration

Review of Inter-Con Security Systems, Inc. Billing Procedures Under the U.S. Department of State Contract No. S-OPRAQ-96-0569 **(01-FMA-M-051)**

At the request of the Office of Inspector General, Leonard G. Birnbaum and Company, certified public accountants, applied certain agreed-upon procedures with respect to Inter-Con Security Systems, Inc. (Inter-Con) billing procedures under U.S. Department of State Contract No. S-OPRAQ-96-0569. The scope entailed the selection of two sets of invoices from those submitted for services rendered between May 12, 2000, and February 16, 2001. The Department awarded the contract to Inter-Con on May 6, 1996. The contract's performance period was from January 6, 1997, through June 5, 2001. Under the contract, Inter-Con provided uniformed armed and unarmed guard services to the Department's Bureau of Diplomatic Security for Department offices and facilities in the greater Washington, D.C., area and other domestic locations. The contract was a time and material contract with an estimated amount of $68 million.

The limited-scope review disclosed the erroneous payment of higher rates than required under the contract for request orders designated as temporary additional services (TAS). Consequently, the Department overpaid Inter-Con several million dollars for work performed under TAS orders. OIG estimated that overpayments could total $4.6 million since the start of the contract.

Review of the Overseas Wireless Program **(01-FMA-M-053)**

OIG reviewed the Department's implementation of the Overseas Wireless Program (OWP). The overall objective of the review was to determine how well the OWP has improved the security environment at overseas posts. The specific objectives were to determine whether: (1) the goals and objectives of the OWP were clear and achievable, (2) posts' Emergency Action Plans (EAPs) effectively integrated the OWP, and (3) the Department assured the best value to the Government in the procurement of products and services. OIG also assessed the Bureau of Information Resource Management's (IRM) compliance with the Government Performance and Results Act of 1993 in implementing the OWP.

The Department initiated the OWP in October 1998 in response to the terrorist attacks on U.S. Embassies Nairobi and Dar Es Salaam and to address prior OIG security inspections that recommended strengthening the Department's overseas radio programs. OIG observed that the OWP program has improved the security environment overseas by creating dedicated Emergency & Evacuation (E&E) radio networks, adding encryption capability as a security enhancement, and providing newer and more robust equipment. IRM officials have generally laid clear goals for the program and have worked vigorously for its implementation. IRM officials have also vigorously incorporated performance measures into the OWP. Officials in the field had differing opinions on how an E&E network with OWP equipment should work and some skepticism that it was even necessary in some posts where risks are perceived as lower. Because the Bureau of Diplomatic Security (DS) controls the local guard program and local guard radios, the OWP program did not address a radio-related security shortcoming that was identified in the Embassy Nairobi bombing. However, IRM and DS should work together to address this shortcoming. The OWP has not always led to fully implemented E&E programs overseas. IRM's plans to perform follow-up visits to OWP posts should help address these concerns, but the regional bureaus and post management must take action as well.

Major recommendations include that IRM reexamine E&E radio distributions to specific posts, and that the regional bureaus stress to posts the importance of fully incorporating E&E procedures concerning the OWP into the posts' EAPs.

Reports Issued Relating to Foreign Policy

Inspection of Embassy Algiers, Algeria **(01-FP-R-046)**

Energy-rich Algeria provides significant opportunities for American diplomacy, but widespread violence in the early 1990s forced the embassy to reduce staff and limit activities. As of early 2001, the capital (but not the countryside) is far safer, and the Department would like to conduct a more normal diplomacy. The embassy, however, is neither equipped nor staffed to do so.

Extensive security precautions are still needed and limit what the embassy can accomplish. The post must also cope with chronic deficiencies in almost all support operations, from housing to basic inventory controls. None of the seven American security officers speaks the French required to facilitate supervision of local personnel. Insufficient radios and cell phones, and the absence of classified e-mail, compound security problems. These shortcomings are unacceptable at a critical threat post. All American personnel live on the embassy compounds, but wide disparities in housing quality lower morale. Housing should be upgraded. Although allowances are generous, it remains difficult to attract experienced personnel. Security constraints and short tours contribute to, but do not excuse, poor performance. For example, there was no inventory reconciliation for eight years. When the post finally reconciled its inventory in 2000, $1.8 million in equipment and supplies were missing.

The number of American direct-hire employees appears adequate for the post's current responsibilities. Of the 35 American employees, 21 are in nonsecurity positions. The Algerian staff forms the backbone of the post, but few had adequate supervision.

Inspection of Djibouti, Republic of Djibouti **(01-FP-R-047)**

Djibouti's port and airport are the primary reasons for American interest in this small country on the Horn of Africa. Both have proven useful in dealing with humanitarian disasters and military contingencies in the region. The U.S. Embassy facilitates access, while France plays a key stabilizing role by stationing 3,000 military personnel in Djibouti. The embassy has nine direct-hire Americans and a budget of $3.5 million. The small, expensive embassy rightly participates in the Special Embassy Program. As long as Embassy Djibouti does not lose sight of why the United States is in Djibouti, management or policy issues should be rare. The decision

to cover the neighboring northwest portion of Somalia (Somaliland) from Djibouti, however, appears to reflect a loss of perspective, including the taking of needless security risks. The Department should assess the advantages and risks of a continued role for Embassy Djibouti in Somaliland. OIG also recommended immediate disposal of a costly, but still unseaworthy, boat used for recreation.

Inspection of Embassy Asmara, Eritrea **(01-FP-R-049)**

United States interests in Eritrea, which achieved independence from Ethiopia in 1993, are largely humanitarian. The post has 22 direct-hire American staff, including a U.S. Agency for International Development mission and two military offices. Designation of Embassy Asmara as part of the Special Embassy Program rightly acknowledges the limited nature of American interests. This isolated post could be more productive, particularly in procurement and commercial work, if it had better Internet access. The chancery compound now has only one Internet terminal. Improved planning can achieve better balance in reporting on key issues.

Reports Issued Relating to Information Technology

More Guidance and Oversight Can Improve Broadcasting Board of Governors' Web Site Privacy **(01-IT-M-039)**

The Internet has emerged as a powerful tool for communicating large amounts of information on Federal activities and services. At the same time, however, the Internet has made it possible for web sites to track and collect personally identifiable data -- such as an individual's name, e-mail address, Social Security number, or credit card number -- making online privacy one of the key and most contentious issues in this information age.

In response to requirements of Section 646 of the Treasury and General Government Appropriations Act, 2001, OIG conducted a review of Internet privacy management at the Broadcasting Board of Governors (BBG). OIG focused the review on the BBG practices regarding the collection of personally identifiable information through the use of "cookies" or other means on its public web sites. A cookie is a small text file placed on a site visitor's computer hard drive by a web server, allowing a server to track online purchases, maintain and serve customized web pages, or build profiles on individual site visitors.

The BBG has not developed policies to ensure that its web sites are managed in accordance with Federal privacy guidelines prescribed by the Office of Management and Budget. Specifically, the guidelines restrict the use of persistent cookies on Federal Internet sites without compelling need, agency head approval, and posted notices to advise the public of any information collected on the sites and how that information is used. The BBG recognizes that it needs to develop web privacy policies to help ensure compliance with Federal Internet management guidelines. Agency officials informed OIG that they recently began to develop a policy directive to ensure compliance with Federal guidelines for Internet privacy management within the International Broadcasting Bureau.

In the absence of agency policies to help ensure web site privacy, OIG found two instances on the four web sites that OIG identified where the BBG was using persistent cookies without proper authorization. In both instances, the web managers did not know that persistent cookies were being used. One of the cookies had been inserted through a commercial web development application as a convenient way of maintaining user preferences (i.e., graphics, screen color) as a user navigates from one web page to another during a site visit. The second cookie was used for counting visitors. Web managers agreed to take steps to remove or seek

BBG approval for the two persistent cookies that OIG discovered during the review. OIG found no evidence that cookies were used to collect personally identifiable information on the agency's public web sites. Further, one of the four web sites that were reviewed had no privacy statement and therefore no means of advising users of any information collected on the site. The web manager was not aware that a privacy statement was required and agreed to post a statement to ensure compliance.

Critical Infrastructure Protection: The Department Can Enhance Its International Leadership and Its Own Cyber Security **(01-IT-R-044)**

The Office of Inspector General reviewed the Department of State's progress in carrying out its Foreign Affairs Lead Agency and critical infrastructure protection responsibilities mandated by Presidential Decision Directive (PDD) 63. The primary purpose was to evaluate the Department's effectiveness in meeting its responsibilities for protecting its minimum-essential cyber infrastructure. The review included an assessment of the Department's PDD-63 Critical Infrastructure Protection Plan (CIPP), vulnerability assessment report, and role as Foreign Affairs Lead Agency. OIG also assessed the Department's risk mitigation, emergency management, interagency security, resources requirements, and awareness and training policies and practices. OIG found that the Department's international outreach approach was commendable; however, it does not address the PDD-63 principles of encouraging friendly and like-minded nations, international organizations, and multinational corporations to focus on cyber security preventative measures. OIG also found that the Department's framework for protecting its minimum-essential infrastructure is workable but needs further improvement to meet the requirements of PDD-63.

Major recommendations for the Department's role as Foreign Affairs Lead Agency include encouraging multilateral cooperation, contingency planning, and open exchange of public information with friendly and like-minded foreign governments. Other recommendations include providing bureaus and posts with public CIPP information to disseminate to foreign governments and encourage U.S. Government lead agencies to inform and assist friendly and like-minded countries to defend themselves effectively against cyber attacks.

Major recommendations concerning the Department's CIPP include addressing foreign operations in subsequent CIPP and vulnerability assessments and conducting security controls evaluations of all minimum-essential cyber infrastructure at least once every three years.

Reports Issued Relating to Security Infrastructure Oversight

During this reporting period, OIG conducted security inspections of Embassy Phnom Penh, Cambodia; Embassy Jakarta, Indonesia; Embassy Hanoi and Consulate General Ho Chi Minh City, Vietnam; and also of U.S. Diplomatic Posts in the Bureau of European Affairs.