United States Department of State
and the Broadcasting Board of Governors
Office of Inspector General

Memorandum Report

Consular Affairs Information Security Program

Report Number IT-A-02-04, September 2002

Decontrolled

MEMORANDUM

TO: CA - Mr. George C. Lannon, Acting

FROM: OIG - Clark Kent Ervin

SUBJECT: Consular Affairs Information Security Program (Report No. IT-A-02-04)

Due to increased risks to information assurance[1] in today's environment, ensuring that security requirements are met in visa and passport processes is essential to national security. The Bureau of Consular Affairs (CA) has responsibility for issuing or refusing visas and passports for the entry of people to the United States.

In response to public and congressional concern about the Department of State's (Department) ability safely to manage and process consular activities, the Office of Inspector General (OIG) conducted a review of CA's information security program. The specific objectives of this review were to determine (1) whether CA's information systems security program complies with statutory and regulatory guidance and (2) whether overseas missions where CA systems operate are following sound information security practices.

This memorandum provides information concerning the first objective. Issues related to the second objective concern mission security management practices, which are not specific to CA. OIG has addressed these issues in its evaluation of the Department's information security program under the FY 2002 Government Information Security Reform Act (GISRA)[2] review.[3]

CA's Comprehensive Approach

CA has developed a comprehensive approach to addressing information security risks. In accordance with GISRA, Clinger-Cohen (P.L. 104-106), and Office of Management and Budget (OMB) Circular A-130, CA provides an overview of its approach to information security in its 1999 Modernized Systems Information Systems Security Plan. The plan establishes organizational authorities and responsibilities to ensure that specified security requirements are met in its client-server environment, currently in production domestically and overseas. The plan also describes:

- CA systems and their operational status;
- the system environment and related software;

[1] Information Assurance is defined as the grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met.
[2] Public Law 106-398, Div. A, Title X, Subtitle G.
[3] *Government Information Security Reform Act, Information Security Program Evaluation* (Report Number IT/A – 02 – 06, September 2002).

- the sensitivity of information handled;
- controls for risk management, security, and rules of behavior;
- operational controls for personal security, contingency planning, hardware and system software maintenance, integrity, and incident response capability; and,
- technical controls for identification and authentication mechanisms, and logical access.

The Consular Systems Division (CSD) oversees the development and dissemination of policies and procedures, ensures the development and presentation of user and contractor awareness sessions, conducts both vulnerability and risk assessments, and inspects and spot checks systems and desktops to confirm that consular sections are in compliance with required security configurations. After an application is deployed to an embassy or consulate, the specific mission takes ownership of applications and the CSD provides 24-hour maintenance and assistance via the deployment teams and the CA Support Desk.

During FY 2002, in coordination with the Bureau of Diplomatic Security, CSD is undergoing a vulnerability assessment of its critical systems and applications. CA management is conducting this initiative to provide assurance that consular information is protected to a level that is commensurate with its sensitivity. The organization conducting the assessment will review and test the applications, database systems, associated network infrastructure controlled or managed by CA, and other controls that are supposed to prevent unauthorized access.

System Survey Results

OIG developed a data collection tool to obtain general information about CA's information security program. The purpose of the tool was to identify the applications used by CA and to obtain information on Information Technology (IT) security plans, assessments, and determinations that are required by OMB guidance, prior information security laws, and also by GISRA. Specifically, the tool included requests for information on the following:

- **Risk Assessments:** The identification and analysis of possible risks in meeting the agency's objectives, which forms a basis for managing the risks identified and implementing deterrents.
- **Security level determinations:** Assessments that identify the specific security levels that should be maintained for IT systems hardware, software, and the information maintained or processed on systems.
- **System Security Plan:** A written plan that clearly describes the entity's security program and the policies and procedures that support it. The plan and related policies should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security as well as those who own, use, or rely on the entity's computer resources.
- **Certification and Accreditation:** Attests that an information system meets documented security requirements and will continue to maintain the approved security posture throughout its life cycle.
- **Tests of security controls:** Assessments of controls designed to protect computer facilities, computer systems, and data stored on computer systems or transmitted via computer networks from loss, misuse, or unauthorized access.

In its response, CA identified an inventory of 36 systems. Of these, officials within the CSD reported that nearly 70 percent of CA systems are operating with a risk assessment. In addition, almost 50 percent of the CA systems are operating with a security level determination and an overall security plan, and have had their security plans tested. Only four systems have been certified and accredited or provided an Interim Authority to Operate (IATO). According to CSD management, they are actively planning, prioritizing and working toward bringing each of their active systems in line with the information security statutes and OMB guidance. See Attachment 1 for complete survey results.

Certification and Accreditation

CA has taken appropriate steps to develop and implement a robust information security program; however, a key element of such a program, certification and accreditation, continues to lag. The certification and accreditation process is designed to certify that information systems meet documented security requirements and will continue to maintain the accredited security posture throughout each system's life cycle. OIG found that only two of CA's 36 systems have been certified and accredited, and two have been granted an IATO. As a result, CA managers lack sufficient information concerning the extent to which their systems are protected against fraud, illegal practices, or mission failure. OIG found that CA management had prepared and submitted the necessary documentation for the certification for eight of 36 CA systems. However, the certifying and accrediting agents for the Department have been unable to complete the process.

The Department's certification and accreditation deficiencies were raised in the OIG's GISRA report in September 2002. Although the Under Secretary for Management has provided support and guidance to the Department's CIO, the Bureau for Diplomatic Security (certification agent) and the Bureau for Information Resource Management (accreditation agent) have not been able to get the process on track as of the date of this memorandum. CA officials told OIG that they are dissatisfied with the process because they continue to submit documented packages for required testing and approval, but must operate their systems without certification and accreditation.

Survey of CA Personnel

Finally, in coordination with CA headquarters, OIG conducted a global survey to measure consular staffs' perception of IT and information security issues. The survey instrument was nonscientific and the data received was subjective. In addition, OIG did not test a random sample of CA personnel nor conduct a validity study on the responses received. However, OIG believes that the results, 993 responses from 124 different missions, provide a useful indicator of information security awareness among CA personnel. For example, 61 percent of respondents said they had received a security briefing in the past 12 months. For complete survey results see Attachment 2.

Please contact Frank Deffer, Acting Assistant Inspector General, Office of Information Technology at (703) 284-2715, or email at defferf@state.gov, if you have any questions or comments.

Consular Affairs Survey Results:
Key Information Systems Security Elements

Consular Applications	Applications with Risk Assessments	Applications with Security Level Determinations	Applications with Security Plans	Applications Certified and Accredited	Applications with Tested Security Controls
American Citizen Services	X	X	X	-	X
Automated Cash Register System	X	X	X	-	X
Action Request System (Domestic) (ARS Remedy-Help Desk)	-	-	-	-	-
Ad Hoc Reporting Template	-	-	X	-	-
Backup Name Check	X	X	-	-	X
Consular Consolidated Database	**	X	X	-	X
Consular Lookout and Support System – Enhanced	X	X	**	-	X
Crisis Report Information System	X	-	-	-	-
Consular Shared Tables	X	X	X	-	X
Consular Workload Statistics System	-	-	-	-	-
Data Share	X	X	**	-	X
Diversity Immigrant Visa Information System	X	-	-	-	-
Independent Name Check	X	-	-	-	-
INS Allocation Management System	X	X	X	IATO	X
International Parental Child Abduction	X	X	X	IATO	X
Immigrant Visa System	X	X	X	X	X
Immigrant Visa Allocation Management System	-	X	-	-	X
Immigrant Visa Information System	X	-	X	-	-
Immigrant Visa/Diversity Visa System	X	X	X	-	X
Knowledge Management System	-	-	-	-	-
Logistics Management System (IRF Inventory System)	-	-	-	-	-
Nonimmigrant Visa System	X	X	X	X	X
Nonimmigrant Visa Ticketing System	X	X	-	-	X
Nonimmigrant Visa Identification Detection Encryption Name Tag System	X	-	-	-	-
Parser System	-	-	X	-	-
Passport Service System	-	X	-	-	X
Passport Records Imaging Systems	-	-	-	-	-
Remote Data Entry System – Client	X	-	-	-	-
Remote Data Entry System – Server	X	-	-	-	-
Remote Outreach Enrollment System	X	-	-	-	-
Refusal Screening and Verification Process	X	-	-	-	-
Structured Query Interface System	X	-	-	-	-
Telecommunications Manager System	X	-	X	-	-
Travel Document Issuance System	X	X	-	-	X
Tracking of Applicants (VISTA)	-	X	-	-	X
Visa Waiver	-	-	-	-	-
Totals	**25 or 69.4%**	**17 or 47%**	**15 or 42%**	**4 or 11%**	**17 or 47%**

** CA's System Security Authorization Agreement (SSAA) in draft, near completion

OIG Global Survey of CA Staff

In coordination with the CA headquarters, OIG conducted a global survey designed to determine consular staffs' perception of IT and information security issues. OIG received 993 responses from 124 embassies and consulates. It is important to note that the survey instrument was not scientific and the data received was subjective. In addition, OIG did not test a random sample of CA personnel nor did OIG attempt to validate the responses. Information on the OIG survey approach and a list of acronyms is provided at the end of this section.

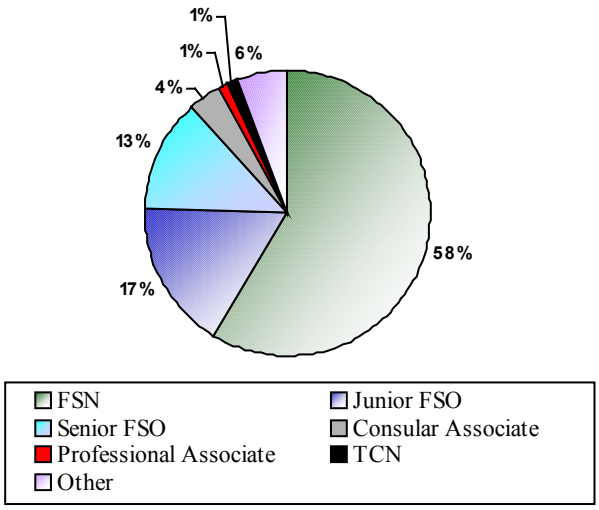
Statistical Description of Respondents

OIG asked all survey respondents to include their position title on their responses. According to CA, there are approximately 950 actual overseas American consular positions. Of the 993 responses that OIG received, 392 responses (41 percent) were from the American consular officer population.

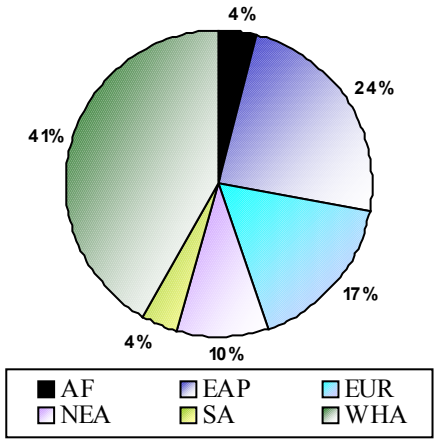
According to CA, there are also approximately 2,700 Foreign Service National (FSN) and Third Country National (TCN) positions. Of the 993 responses that OIG received, 595 responses (22 percent) were from the FSN/TCN population.

OIG also asked all survey respondents to include their mission. Identifying the mission allowed OIG to calculate the consular section's size[4] and regional bureau in a reliable and valid manner.

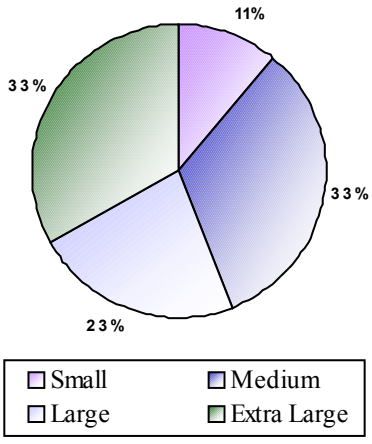
Positional Responses



Regional Responses



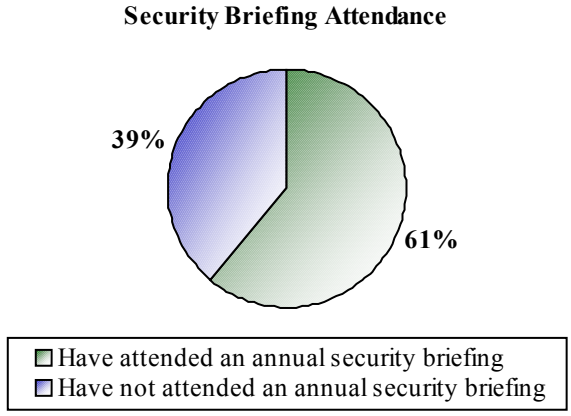
Mission Size Responses



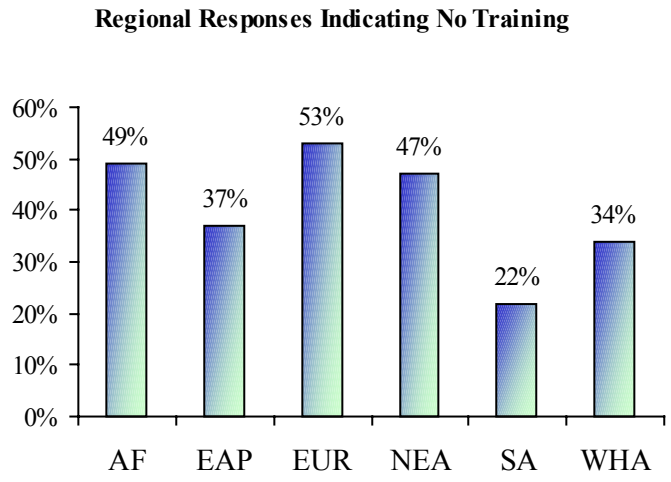
[4] Mission size was based on a CA-generated formula that factors in the number of visa and passport cases, turnover of personnel, physical hardships at posts, level of expertise along with other general factors.

Information Technology Security Briefings

OIG asked survey participants to say whether they had attended at least one IT information security briefing within the last 12 months. Of the responses received, 39 percent said that they had not been briefed within the last year. This is significant because training and awareness are key elements in reducing risk and enhancing the Department's risk-based management approach for IT security.



More specifically, the greatest range of responses to this question was evident in the regional bureaus. For example, 78 percent of respondents in the Bureau of South Asian Affairs (SA) said that they had received at least one security briefing within the past 12 months. In contrast, only 47 percent of the respondents from the Bureau of European and Eurasian Affairs (EUR) said they that they had received a security briefing within the past 12 months.

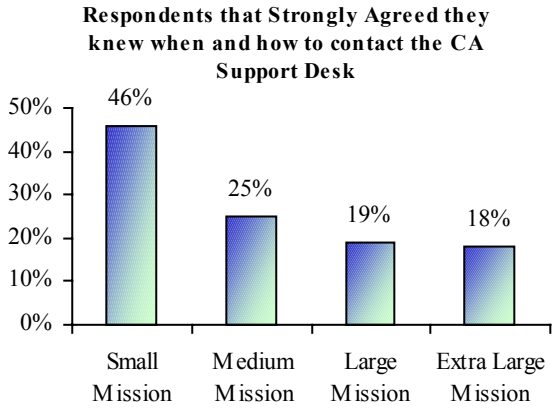


Number of responses that said attendance at least one security briefing in the last 12 months:
Yes: 384 **No:** 609

CA Support Desk

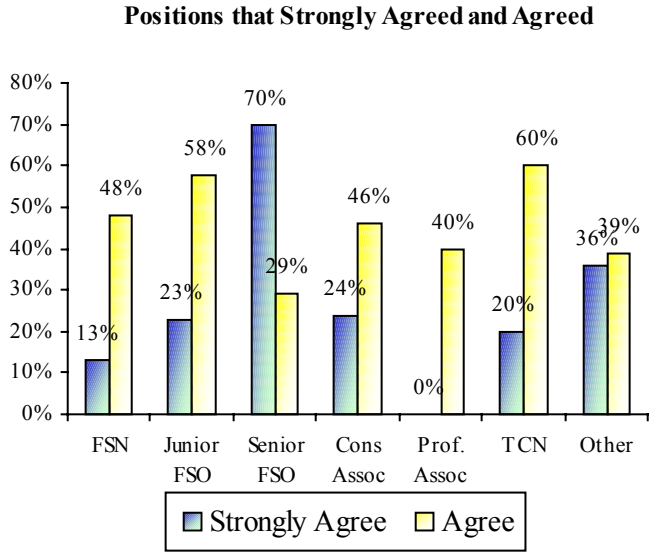
The CA Support Desk, staffed 24 hours a day, is the primary channel through which CSD provides maintenance and support to CA applications.

OIG asked respondents to say whether they strongly agreed, agreed, disagreed, or strongly disagreed with the suggestion that they knew when and how to contact the CA Support Desk.



Almost 24 percent of the respondents strongly agreed that they knew when and how to contact the CA Support Desk. More broadly, over 70 percent of all respondents said that they either strongly agreed or agreed that they knew when and how to contact the CA support Desk.

Respondents from smaller missions were more likely strongly to agree. For example, 46 percent of the respondents from small missions submitted a strongly agree response. In contrast, only 18 percent of respondents from extra large missions said that they strongly agreed.

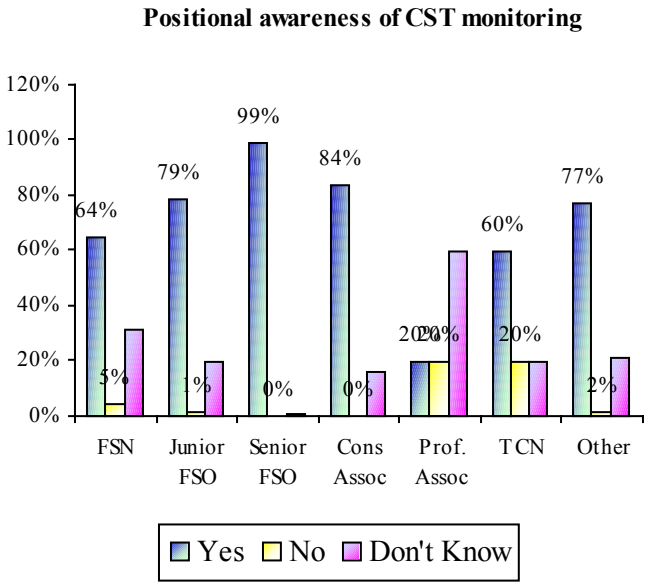


OIG also saw a significant range within positions. For example, almost 70 percent of senior Foreign Service Officers (FSO) said that they strongly agreed that they knew when and how to contact the CA Support Desk. In contrast, only 13 percent of the FSNs said knowledge of when and how to contact the Support Desk.

Number of responses that said that they had knowledge of when and how to contact the CA Support Desk:
Strongly Agree: 234; **Agree:** 459; **Disagree:** 158; **Strongly Disagree:** 30; **NA:** 106

Consular Shared Tables

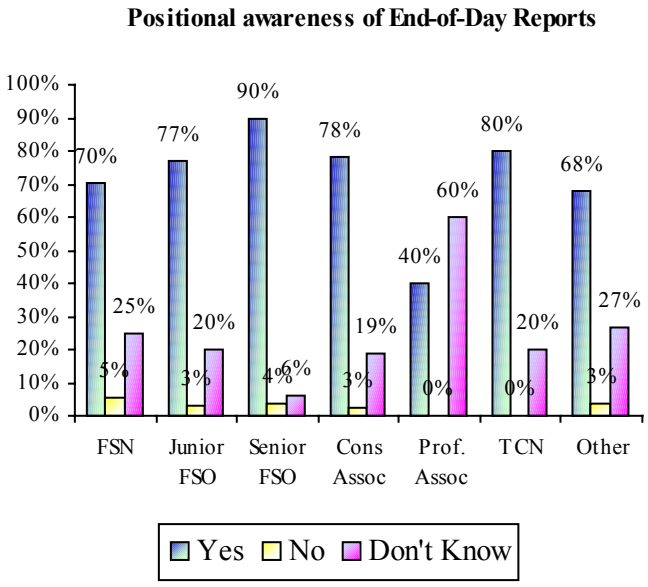
Survey participants were asked whether they were aware of their consular section's Consular Shared Tables (CST) manager actively assigning and monitoring user IDs and roles within the Consular Shared Tables. Of the responses received, 73 percent said that they were aware that the CST were regularly monitored. OIG also asked respondents how often CST tables were monitored. According to 47 percent of senior FSOs, the tables are monitored every month, and 41 percent said that they were monitored every six months.



Number of responses that said someone in their consular section regularly monitored user roles and identifications in CST:
Yes: 716; **No:** 32; **Don't Know:** 239

End-of-Day Reports

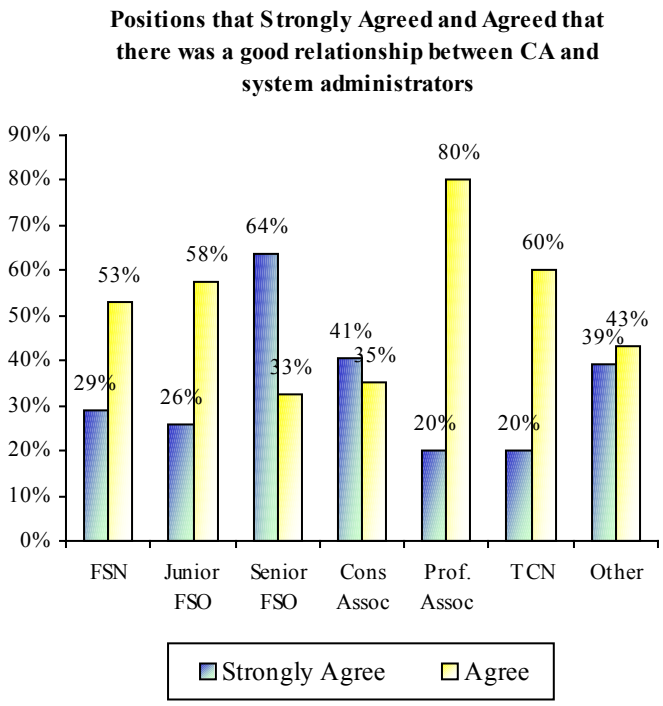
OIG asked survey participants whether anyone in their mission's consular section consistently monitored and reviewed end of day reports relevant to their mission. In response, almost 90 percent of senior FSOs said that end of day reports were reviewed.



Number of responses that said someone in their consular section used end of day Reports:
Yes: 730; **No:** 45; **Don't Know:** 212

Working Relationship between CA and IM

OIG asked survey participants to say whether they thought that their mission's consular managers had a good working relationship with the systems support personnel. Overall, over 80 percent of total respondents either strongly agreed or agreed that their consular section and systems support personnel had a good working relationship. OIG found the largest range in answers in positions. For example, 64 percent of senior FSOs strongly agreed that there was a good working relationship between their section and the system administration. However, only 26 percent of the junior FSOs shared that opinion.

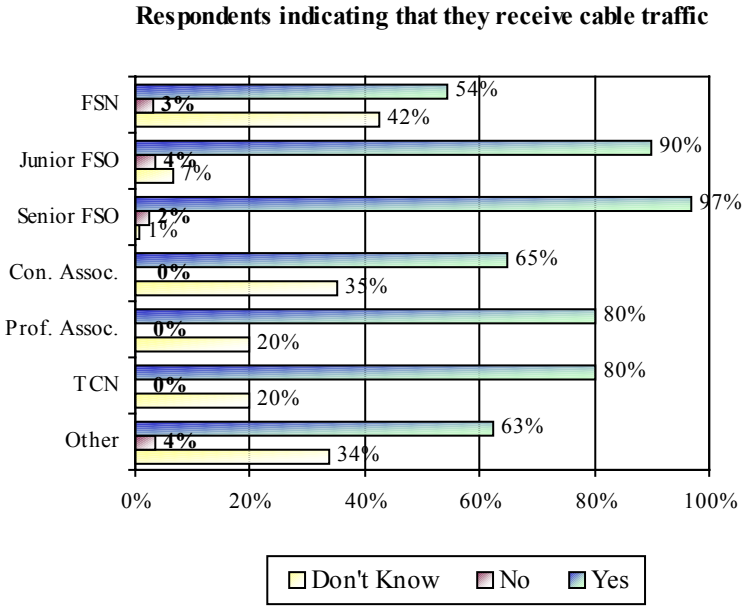


Number of responses indicating a good working relationship between CA staff and system administrators:
Strongly Agree: 334; **Agree:** 494; **Disagree:** 21; **Strongly Disagree:** 5; **Don't Know:** 132

Cables

CSD said that they were interested in knowing whether their missions receive cable traffic, such as monthly cables or information on new software releases.

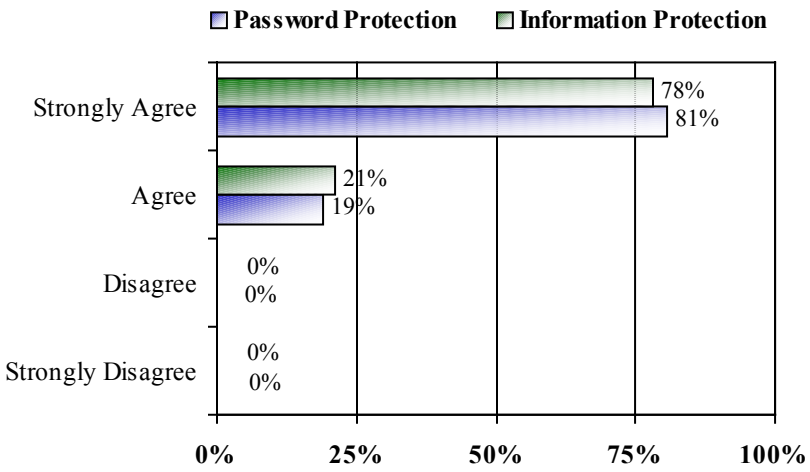
When OIG asked all survey participants whether they regularly received cable traffic, 67 percent said that they were aware of cable traffic from headquarters. According to the responses, the smaller the mission, the more likely the respondents were to be aware of cable traffic.



Number of responses that said that their mission regularly received cable traffic:
Yes: 659; **No:** 31; **Don't Know:** 296

Protection of Information Technology Passwords and Consular Information

OIG asked survey participants whether they understand that their IT password(s) are not to be shared with other persons. In addition, OIG asked survey participants whether they understand that consular information is protected by the Privacy Act and that it is everyone's responsibility to protect these records from release to persons outside of the Department. Almost 100 percent of respondents said that they either strongly agreed or agreed that they understand the importance of protecting both their passwords and consular information.

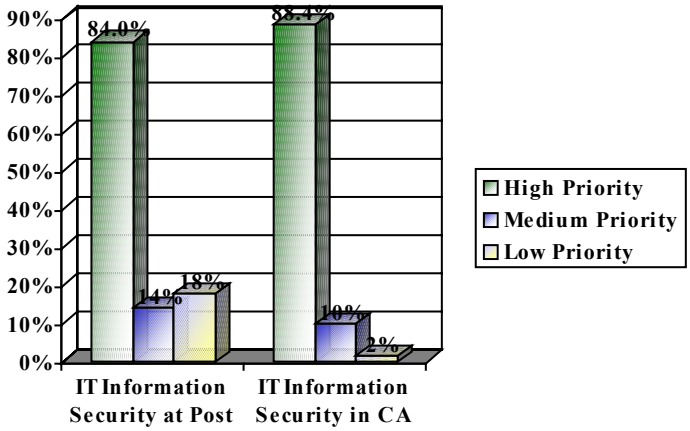


Number of responses indicating that employees understand the importance of password protection:
Strongly Agree: 665; **Agree:** 155; **Disagree:** 3; **Strongly Disagree:** 1; **Don't Know:** 132

Number of responses indicating that employees understand the importance of information protection:
Strongly Agree: 644; **Agree:** 175; **Disagree:** 4; **Strongly Disagree: 1**; **Don't Know:** 132

Information Technology Security Priorities

Finally, OIG asked survey participants to rank their perception of IT security's priority in the mission as a whole and the consular section. In both scenarios, 98 percent of participants said that they thought that IT information security was a medium or high priority.



Number of responses ranking the priority of IT security in the mission:
High: 830; **Medium:** 139; **Low:** 18

Number of responses ranking the priority of IT security in the consular section:
High: 873; **Medium:** 99; **Low:** 15

Survey Approach

The survey was made available on the CA Intranet site from May 25 through July 11, 2002. A cable was distributed to all diplomatic missions and consulates inviting consular staff to participate in the survey. For more information on this survey, please call Heather Rogers at (703) 284-2732 or send an e-mail to rogersh@state.gov.

Acronym List for OIG Global Survey to CA Staff

AF	Bureau of African Affairs
CA	Bureau of Consular Affairs
CSD	Bureau of Consular Affairs, Consular Systems Division
CST	Consular Shared Tables
EAP	Bureau of East Asian & Pacific Affairs
EUR	Bureau of European and Eurasian Affairs
FSN	Foreign Service National
FSO	Foreign Service Officer
IT	Information Technology
NEA	Bureau of Near Eastern Affairs
OIG	Office of Inspector General
SA	Bureau of South Asian Affairs
TCN	Third Country National
WHA	Bureau of Western Hemisphere Affairs